worldpay

Important Information

Customer Operating Instructions

Please Note: Customer Operating Instructions are referred to as the Merchant Operating Instructions in our contractual arrangements

Table of Contents

1 Welcome 6

1.1 Making the most of this guide 6

1.2 What else you need to read 6

1.3 Your customer number 6

1.4 Point-of-sale display material 7

1.5 If you need to contact us 7

2 Important Information 10

2.1 Your contract with us 10

2.2 Terminating your acquiring contract 10

2.3 You must tell us about any of these: 10

2.4 Your terminal is for business use only 11

2.5 Minimising risk 11

2.6 Card types 11

2.7 Keeping records 11

2.8 Using your terminal 11

2.9 Authorisation of transactions 12

3 Payment And Information Security 13

3.1 PCI DSS Levels 13

3.2 Obligations of your service providers if you do not store card data on your own systems 15

3.3 Level 1, 2 and 3 Customers 15

3.4 Staying compliant 17

3.5 General security information 18

4 Card Present Transactions 19

4.1 Chip and PIN and Contactless 19

4.2 When a signature is needed 20

4.3 Troubleshooting 21

4.4 American Express 22

5 Authorisation And Referrals 23

5.1 Making a referral call 23

5.2 Suspicious transactions 24

5.3 Transaction changes after authorisation and before processing 24

© Worldpay 2015. All rights reserved

5.4 Split transactions 24
6 Refunds 25
6.1 Before making a refund 25
6.2 Making a refund using your terminal 25
6.3 Making a refund using paper vouchers and the manual imprinter 25
6.4 American Express refunds 26
7 Purchase With Cash Back 27
7.1 To offer Purchase With Cash Back: 27
7.2 Before you start 27
7.3 A step-by-step guide 27
8 Terminal Failure 29
8.1 Using paper vouchers 29
8.2 Before you start 29
8.3 A step-by-step guide 29
8.4 Making a refund using paper vouchers 30
8.5 Processing paper vouchers 30
9 Card Not Present Transactions 32
9.1 Can I accept CNP transactions? 32
9.2 Authorisation 32
10 Mail Order And Telephone Order 33
10.1 Which cards can I accept? 33
10.2 Reduce the risk of fraud 33
10.3 What details do I need from the cardholder? 33
10.4 The Data Protection Act 1998 34
10.5 How to complete a MOTO transaction 34
10.6 Additional security checks for MOTO transactions 34
10.7 Making an informed decision 37
10.8 Protect your business 37
10.9 Delivery, documents and record-keeping 37
11 eCommerce Transactions 38
11.1 Important 38
11.2 Payment types you can accept 38
11.3 Reducing fraud and chargebacks 38

© Worldpay 2015. All rights reserved

11.4 Cancellations after an eCommerce order is taken 39
11.5 Keeping customer data secure 39
11.6 Cardholder Authentication 39
11.7 If you change your payment service provider (PSP) 40
11.8 Guidance notes 40
12 Recurring Transactions 42
12.1 The basics 42
12.2 Obtaining written authority 42
12.3 Recurring transaction options 43
12.4 Cancellation 43
12.5 Important information for eCommerce customers 43
13 Reducing Fraud 45
13.1 Always remember 45
13.2 Training your staff 45
13.3 Card present transactions 46
13.4 Card Not Present Transactions (CNP) 49
14 Reconciling Your Invoice 53
15 Chargebacks 55
15.1 Why chargebacks happen 55
15.2 What if cardholders get in touch with you directly? 56
15.3 What is a Request For Information (RFI)? 57
15.4 Secure record keeping 58
15.5 If the post is disrupted 58
15.6 Disputing a chargeback 58
16 Our Other Services 59
16.1 Hotel Services 59
16.2 Vehicle Rental Services 62
16.3 Bureau de Change 66
16.4 myCurrency 67
16.5 Tax free shopping 67
17 Card Recognition Guide 68
17.1 Not a chip and PIN card or Contactless card? 68
17.2 Key security features 68

© Worldpay 2015. All rights reserved

17.3 Example of cards 68
17.4 What to look out for? 69
17.5 Visa combination cards 71
17.6 Examples of card UV images 71
18 Terminology 72

This document and its content are confidential and proprietary to Worldpay and may not be reproduced, published or resold. The information is provided on an "AS IS" basis for information purposes only and Worldpay makes no warranties of any kind including in relation to the content or sustainability. Terms and Conditions apply to all our services.

Worldpay (UK) Limited. Registered in England No. 07316500. Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AF. Worldpay (UK) Limited is authorised by the Financial Conduct Authority under the Payment Service Regulations 2009 (No. 530923) for the provision of payment services and is authorised and regulated by the Financial Conduct Authority for consumer credit activities. Worldpay, the logo and any associated brand names are all trademarks of the Worldpay group of companies.

© Worldpay 2015. All rights reserved

1 Welcome

Thank you for choosing to accept payments with Worldpay. As one of the world's leading payment companies we manage millions of payments every day and make it easy for businesses like yours to enjoy the full advantages of accepting cards and other non-cash payments.

With Worldpay, you will benefit from market-leading flexible products; a dedicated Helpdesk available 365 days a year and personal service that meets the individual needs of your business.

1.1 Making the most of this guide

This guide will help you make the most of the benefits of accepting payments with Worldpay. Please read this guide carefully, as it will help you to:

- Accept card payments efficiently and smoothly
- Receive prompt payments to your bank account
- Protect your business by minimising the risk of losses caused by fraud and mistakes
- Understand your responsibilities

The contents of this guide also form a part of your contract with Worldpay.

1.2 What else you need to read

To make sure you have all the information you need, you should read this guide together with:

- Your Worldpay Terms and Conditions, and any variations since issued.
- Your Terminal User Guide
- Any prompts displayed on your payment terminal
- Any updates and specific instructions we send you in the future

1.3 Your customer number

When you join Worldpay you will receive a unique Customer Number, which you will need to quote whenever you write to us or call the Worldpay Helpdesk or Authorisation Centre.

Never give your Customer Number to anyone else: no-one from Worldpay will ever call you to ask you for this number.

Note: The Customer Number may also be referred to as the Merchant ID or MID.

© Worldpay 2015. All rights reserved

1.4 Point-of-sale display material

Before you begin to accept card payments you will need to take a few steps to ensure your customers are aware that they can use them at your shop or business.

A well-designed point-of-sale (POS) display encourages increased spending. We can provide display materials for your business to show your customers that you accept card payments.

These include:

- Shop-front window and door stickers
- Stickers for shelving and the back of tills
- 'Tent-style' cards to put on the counter or on restaurant tables

Order point-of sale display material online or call us. See section 1.5. for contact numbers

1.4.1 Using card symbols in sales material

You can also use card symbols and logos in your own marketing material and websites. If you'd like to do this, we can supply:

- Artwork examples
- Design guidelines and rules for the individual card symbols and logos
- Pantone™ numbers for colours
- Artwork as computer files for print or web use

Important

The Card Scheme names – MasterCard, Visa, Visa Electron, JCB, Diners/Discover and Maestro – and their associated symbols and logos are registered trademarks. As one of our customers, you are allowed to use the symbols and logos in your advertising, as long as you follow the guidelines we provide. If you want to use American Express you must ask them directly for permission.

1.5 If you need to contact us

This guide should answer most of your questions about processing transactions. However, if you need any further help, please get in touch. We are open 24 hours a day.

1.5.1 AUTHORISATIONS – Cardholder Present Transactions

- **UK customers:** 0845 7 600 500 *
- **ROI customers:** 1 800 700 100

1.5.2 AUTHORISATIONS – Cardholder Not Present Transactions

- **UK customers:** 0845 7 600 530*
- **ROI customers:** 1 800 700 300

1.5.3 NAME AND ADDRESS CHECKS

- **UK customers:** **0845 300 7929**
- **ROI Customers** **1800 700 300**

© Worldpay 2015. All rights reserved

1.5.4 WORLDPAY HELPDESK

Please make sure you have your Customer Number available when calling.

- **UK customers:** 0845 7 61 62 63* (Text phone users may call 18002 0845 761 6263*)
- **ROI customers:** 1 800 24 26 36 (or National 01 702 5845)

*Note: Max call charge from a BT landline is up to 6p per minute. Calls from other networks may vary. Calls may be recorded for training and security purposes.

The Worldpay Helpdesk has a touch-tone telephone system. If you key in the option required on your telephone keypad, whenever you can, you will generally get a faster response than waiting for the 'no selection' option.

Option 1 - Customer Services

The Customer Service sub-options are:

1. Settlements, Invoicing and Processing – If you require assistance to reconcile your terminal totals, Worldpay invoice or a banking entry generated by Worldpay.
2. Chargebacks – If you have a query regarding a chargeback (disputed card transaction) or are responding to a Request For Information.
3. Authorisation Code – PLEASE NOTE: Authorisation cannot be obtained via the Worldpay Helpdesk. You will hear a recorded message reminding you of the number to call for Authorisation service. See section 1.5. and 1.5.2 for authorisation contact numbers
4. Stationery orders including terminal tally rolls.
5. Any other enquiry

Option 2 – Terminal Support (Worldpay Supplied)

The Terminal Support sub-options are:

1. Terminal Fault or Installation query – if your terminal is supplied by Worldpay. PLEASE NOTE: If your terminal is not supplied by Worldpay, you should contact your provider directly.
2. New order or a site visit
3. All other terminal-related enquiries.

Paper Tally Rolls For Card Payment Terminals

If you need more terminal tally rolls for your terminal, you do not need to contact the Worldpay Helpdesk. Instead you should contact the Worldpay approved supplier below or log on to the Worldpay accessories and stationery website:

- **UK customers:** 0800 289 666 (Freephone) or http://worldpay.ncr.com/index.jsp
- **ROI customers:** 00800 9899 2000 (International Freephone)

1.5.5 ECOMMERCE HELPDESK - Existing eCommerce Customers

- **UK customers:** 0870 366 1233
- **ROI customers:** +44 870 366 1233 (international Freephone)

1.5.6 NEW SALES

- **UK customers:** 0808 253 0519 (Freephone) or 02890-099201 from Northern Ireland
- **ROI customers:** 04890 099 201

© Worldpay 2015. All rights reserved

1.5.7 OTHER WAYS TO CONTACT US

We are also available on the website www.worldpay.com

To contact Worldpay in writing, please write to:

Worldpay
Gateshead Card Centre
Victory House
5th Avenue
Gateshead
NE11 0EL
United Kingdom

1.5.8 WORLDPAY COMPLAINT PROCEDURE

The Worldpay Helpdesk team will be pleased to provide help. Details of our Complaints Procedure are available on our website

© Worldpay 2015. All rights reserved

2 Important Information

It is very important to read this information before you start taking card payments because it tells you more about your obligations. If you have any questions, please get in touch with us and we will be happy to help. Find out more about How to Get in Touch - see section 1.5

2.1 Your contract with us

This guide forms part of your Contract with us. It covers the services you have requested and may include some others. Your application form (which also forms part of your Worldpay Contract) shows which services you have requested.

You must ensure that your card processing facility is only used to accept payments for the goods and/or services that you told us your business provides, as detailed in your application form. Taking card payments for goods and/or services without the knowledge and prior agreement from Worldpay may result in termination of your Contract with us.

If you have any doubt about your contractual obligations after reading this guide, we recommend you obtain legal advice.

2.2 Terminating your acquiring contract

If you have no more than ten employees and an annual turnover and/or balance sheet below €2 million then you can give us one month's notice at any time to terminate your Worldpay contract for acquiring services. For customers who do not fit within this criteria, or where we have agreed to provide you with other products of services, different contracts lengths and termination rights may apply. Please review your contract/s carefully.

If we terminate we will give notice as set out in your applicable Worldpay Contract.

2.3 You must tell us about any of these:

- If you change the nature of your business – for example, if you start selling a different kind of goods or services, begin trading online or offer guarantees or warranties
- If you change your website address and/or intend to sell via a new website address.
- If you change the length of the guarantees or warranties offered on your products
- If you change the legal entity of your business – for example from sole trader to limited company
- Change to your bank account details
- Change of postal address
- Change of email address
- Change of contact name
- Change of contact number
- If a partner/director/owner changes name
- If a partner/director leaves or a new partner/director joins
- If you open or close an outlet/site
- If you do not want to take cards any more

You must provide notification to Worldpay of any changes to your circumstances, in writing and with an authorised signature. See section 1.5 for our contact details . If you do not let us know about any of the above changes, we may suspend or withdraw some or all of your card-processing facility.

© Worldpay 2015. All rights reserved

2.4 Your terminal is for business use only

You must not process any transactions that do not directly relate to the sale of goods and services provided by your business and for which you have a contract with us. You must never process transactions on behalf of third parties. This includes sales, Purchase With Cash Back (PWCB) or refunds to your own card account or any other card. If you do not comply with your obligations, we may suspend or withdraw some or all of your card processing facility. We may also suspend or withhold some or all funds for the transactions processed through the facility. In addition you will also be liable for any Card Scheme fines in result of your actions. It is your responsibility to ensure that all of your employees comply with their obligations.

2.5 Minimising risk

You take card payments at your own risk. Risks can exist with all types of card payments but some are higher than others (for example, cardholder not present transactions). This document includes tips on how you might identify and reduce the risk of fraudulent transactions.

If you and your staff follow the instructions in this guide carefully, the risk may be reduced, but it's important to understand that card payments are not guaranteed and that you carry the risk of chargebacks for fraudulent transactions. Even if a payment is authorised this simply means that **at the time of the transaction**, the card had not been reported as lost or stolen (perhaps because the genuine cardholder was not even aware of this at the time) and there were sufficient funds available to cover the transaction. Please make sure that everyone taking card payments for your business has read this guide thoroughly and practised the procedures. We also recommend you hold regular training sessions with all your staff to refresh their understanding.

Much of the information and guidance provided in these Customer Operating Instructions (COI) is based on what we believe is current industry best practice. We hope that such practices will help you minimise possible exposure to security breaches or losses through fraud and chargebacks. **However, Worldpay (and any affiliated companies, representatives, etc.) does not guarantee that security breaches or losses will not happen and will not be held liable in any such cases**.

2.6 Card types

Remember you can only accept card types set out in your Worldpay Contract. If you process any others, the transaction may be returned unpaid, either rejected during processing or returned via the chargeback process.

2.7 Keeping records

Terminal receipts, paper vouchers and other transaction records are high-security items and access to them should be restricted. Keep your copies of all transaction details in a secure fireproof place for at least 13 months in case there is a query later or the details are required to help to defend a chargeback.

Do not alter transaction records in any way. If there is a dispute, the cardholder's copy will normally be taken as correct. After 13 months, make sure that you dispose of all transaction records securely.

See the Payment And Security section for more details of data security requirements.

2.8 Using your terminal

Depending on your terminal type, you may be required to provide a telephone line or internet service for your terminal to connect with the Worldpay Processing and Authorisation Systems. If your terminal is supplied by Worldpay you must ensure that it is connected and powered on at all times to ensure it is available to receive important updates if required. Worldpay provided terminals typically dial Worldpay's host terminal system after

© Worldpay 2015. All rights reserved

every 28 days via a non-geographical telephone number. Please refer to your telephone provider for details of non-geographical call rates.

Mobile terminals operate over GPRS (mobile data network). Whilst normal mobile phone connectivity is a good indicator of service, GPRS coverage and connectivity cannot be guaranteed.

2.9 Authorisation of transactions

Authorisation of a transaction confirms that at the time the transaction was taken the card has not been reported as lost or stolen and there are sufficient funds available to cover the transaction. **It does not confirm the authenticity of the card presenter or the card, nor does it guarantee payment. Find out more about Authorisation and referrals in Section 5.**

© Worldpay 2015. All rights reserved

3 Payment And Information Security

The Card Schemes have set out mandatory information security requirements to help make sure that sensitive cardholder information remains safe including while storing, processing and transacting cardholder data. The requirements are regulated by the PCI Security Standards Council (PCI SSC), formed by Visa, MasterCard, American Express, JCB and Diners/Discover.

All customers must comply with these requirements and certify compliance annually. As a card acquirer, WorldPay has a responsibility to report our customers' PCI DSS compliance status to the Card Schemes (including Visa & MasterCard) on a quarterly basis.

Any customer who does not comply or have not yet begun working towards compliance may run the risk of fines being levied by the Card Schemes, as with any breach of Card Scheme rules (in addition to any monthly non-compliance and other service fees that we may charge). In addition, customers who suffer a data breach may be subject to fines being levied by the Card Schemes for the loss of card data, associated fraud spend, loss of business and reputation. There are also fines for storing Sensitive Authentication Data (SAD) post- authorisation e.g. the 3 digit security code on the back of the card.

In addition to confirming your compliance annually, it is equally important to ensure that this degree of protection is maintained long term. PCI DSS is intended to protect your business and customers against real data security risks – it is not a box ticking exercise.

3.1 PCI DSS Levels

Customers are classified between PCI level 1 – 4 depending on the nature of their business and volume of transactions processed. See below for details of the levels and associated PCI accreditation requirements. You can find a step by step guide for Levels 1-3 in section 3.3 below.

For Level 4, customers can use Worldpay's SaferPayments programme to confirm compliance with PCI DSS. SaferPayments has been designed to give these businesses a helping hand through the Payment Card Industry Data Security Standard (PCI DSS) certification process. Further details can be found below.

Level 1 – Customers processing more than 6 million Visa or MasterCard transactions a year

- Annual on-site audit carried out by a Qualified Security Assessor (QSA), providing a Report on Compliance (ROC)
- Quarterly vulnerability scan by an Approved Scan Vendor (ASV)
- Attestation of Compliance Form

Level 2 – Customers processing between 1 and 6 million Visa or MasterCard transactions a year

- Annual Self-Assessment Questionnaire (SAQ)
- Quarterly vulnerability scan by an Approved Scan Vendor (ASV)
- Attestation of Compliance Form – part of the Self-Assessment Questionnaire (SAQ)

Level 2 customers that choose to complete an annual self assessment questionnaire must ensure that staff engaged in the self assessment attend PCI SSC Internal Security Assessor training and pass the associated accreditation programme annually in order to continue the option of self assessment, for compliance validation. Alternatively, Level 2 customers may, at their own discretion, complete an annual onsite assessment conducted by a PCI SSC approved qualified security assessor (QSA) rather than complete an annual self assessment questionnaire.

© Worldpay 2015. All rights reserved

Level 3 – Any customer processing 20,000 to one million Visa or MasterCard ecommerce transactions per year.

- Annual Self-Assessment Questionnaire (SAQ)
- Quarterly vulnerability scan by an Approved Scan Vendor (ASV) – if applicable
- Attestation of Compliance Form – part of the Self-Assessment Questionnaire (SAQ)

Level 4 –

E-commerce customers only - Any customer processing less than 20,000 Visa or MasterCard e-commerce transactions per year

Non e-commerce customer - Any customer processing up to one million Visa or MasterCard transactions per year.

- Annual Self-Assessment Questionnaire (SAQ) (recommended)
- Quarterly vulnerability scan by an Approved Scan Vendor (ASV) (if applicable)

Worldpay's SaferPayments Programme is available for Level 4 customers to help them through the process of certifying compliance with PCI DSS. To find out more visit www.worldpay.com/uk/saferpayments.

SaferPayments are open weekdays from 8am to 10pm and weekends from 9am to 5pm.

UK 0845 874 0374
ROI 1890 989 575

3.1.1 About the annual on-site audit

The annual on-site audit is an independent risk assessment, usually carried out by a Qualified Security Assessor (QSA), who will follow a standard testing procedure, built around the 12 PCI DSS requirements.

If you currently use a security consultant to do on-site reviews, they may be able to carry out the PCI DSS on-site audit. It may also be possible for the audit to be carried out by your own staff.

To find out more, visit our SaferPayments website.

3.1.2 About the quarterly vulnerability scan

A vulnerability scan checks that your IT systems are protected from external threats, such as hacking or malicious viruses. The scanning tools test your network equipment, hosts, and applications for known vulnerabilities. Scans are intended to be non-intrusive, and are conducted by an authorised network security scanning vendor.

Regular quarterly scans are necessary to check that your systems and applications continue to provide adequate levels of protection. If the scans identify any vulnerability, you will need to address these and carry out a follow-up scan to ensure that the remediation was successful.

For a current list of providers, go to the PCI Security Standards Council Website

© Worldpay 2015. All rights reserved

3.2 Obligations of your service providers if you do not store card data on your own systems

Even if you do not store any cardholder account data in your own systems, you will still need to verify the PCI DSS status of any third parties who act on your behalf to store, process or transmit your customers' cardholder data. In accordance with the relevant PCI DSS requirements, you are responsible for monitoring the PCI DSS compliance of all third party service providers you use who have access to cardholder data (including to possess, store, process or transmit it on your behalf), and/or who could impact the security of your cardholder data environment. Third-party service providers may include:

- Resellers
- Software application providers
- Acquirers
- Payment service providers (PSPs)
- Card processing bureaux
- Data storage entities
- Web hosting providers
- Shopping cart providers
- Miscellaneous third-party agents
- Software vendors

3.3 Level 1, 2 and 3 Customers

3.3.1 A step-by-step guide

To implement PCI DSS you will need to:

- Find out more about the way your business handles card payments
- Determine whether your business handles cardholder data securely
- Put a remediation plan in place to address any associated data security risks

This step-by-step guide will help you to do this in a way that is manageable for your business.

PCI DSS is intended to protect your business and customers against real data security risks – it is not a box ticking exercise.

3.3.2 Step 1: Get to know PCI DSS

Your first step should be to read and understand the full details of the Payment Card Industry Data Security Standard (PCI DSS) and its 12 requirements. To see the full and latest version, visit our SaferPayments website.

3.3.3 Step 2: Map all data flows in your business

Once you are familiar with PCI DSS, we recommend you put a project team in place within your business. This team's immediate priority should be to analyse the way that card payments are processed in your business and to map out all the related data flows.

This analysis must:

- Identify any systems which store cardholder data
- Identify which of these systems are under your direct control

Depending on the size and type of your business, at least some of these systems may be under the control of a third-party service provider or vendor – such as a till vendor, a POS vendor, an integrated solution provider, an Internet Payment Service Provider, a payment gateway provider or a web hosting company., Your business will be responsible for the activity of these service providers. **All third-parties who are**

© Worldpay 2015. All rights reserved

involved in the handling of cardholder data need themselves to be compliant with the requirements of the Data Security Standards.

Once you have completed Step 2, you should be in a position to:

- Ensure all your service providers comply with PCI DSS
  - To find out more, go to Step 3.
  - If you do not work with any service providers, go straight to Step 4.
- Implement PCI DSS compliance within your own business

To find out more, go to Step 4.

3.3.4 Step 3: Check and monitor the status of your service providers

You are responsible for monitoring the PCI DSS compliance of all third party service providers you use who have access to cardholder data (including to possess, store, process or transmit it on your behalf), and/or who could impact the security of your cardholder data environment.

If data becomes compromised by a service provider you work with, you may be held responsible for any associated costs.

Because cardholder data security is so important for the payment card industry, it is likely that your service providers will know about PCI DSS. Many service providers are already compliant; others have a formal programme in place to become compliant. Service providers should register to complete their PCI DSS compliance.

For a current list of service providers that are compliant or working towards compliance, see 'Procedures and Guidelines' on the PCI SSC website.

If your service providers are not on this list, you need to ensure that they take action toward becoming compliant.

Worldpay may seek your support and intervention during Step 3. For example, we may ask you to put additional pressure on a particular service provider – including by obtaining written confirmation that they are compliant with the PCI DSS requirements.

3.3.5 Step 4: Conduct a gap analysis and scope the project

Having mapped out the data flows in your business, you should have identified any of your systems that store, process or transmit cardholder data. With these systems as your primary focus, you should:

- Assess how much remediation work may be required to comply with PCI DSS
- Assess what resources are needed, and how long this work is likely to take
- Consider putting a project team in place and discuss respective roles and responsibilities – including communicating with us and your service providers, specifying technical changes, establishing training needs, etc.

At this stage you should consider whether to engage the services of a Qualified Security Assessor (QSA) – a specialist auditor, certified by Visa and/or MasterCard to help you achieve PCI DSS compliance. Some customers appoint a QSA from the outset. Others prefer to carry out the initial scoping work internally and bring in a QSA later for a more thorough review.

For a current list of QSAs, visit the PCI SSC website.

3.3.6 Step 5: Select your validation option

Depending on the size of your business and how your card acceptance systems are set up, there are different ways in which to test and validate your compliance with PCI DSS.

Visit the PCI SSC web site for further details

© Worldpay 2015. All rights reserved

3.3.7 Step 6: Plan and implement remediation

Once you have decided on your validation option, you will probably need to carry out a more thorough gap analysis and develop a full remediation plan to become PCI DSS compliant.

This can be done by your own team, or you could appoint a Qualified Security Assessor (QSA) to provide an independent perspective on your remediation plan.

At this stage, you should give the individual members of your project team specific remediation activities and agree acceptable timelines. Some activities may depend on a third party or vendor becoming compliant, whilst others can be undertaken internally. From a project management perspective, it may seem better to wait until any service providers become compliant, but it's important to remember that the underlying aim of PCI DSS is the security of your business and of customers' data, not the compliance process.

Because of this, we recommend that you begin any remediation work on your own systems as quickly as possible. By doing whatever you can as soon as you can, you will be taking a vital step forward in protecting your business and customers against the risk of data compromise.

3.3.8 Step 7: Certification

In order to go through the final certification stage, your business will need to:

- Complete the remediation of all systems under your control
- Confirm that all your service providers are fully compliant – and that their compliant products and services have been implemented within your own card acceptance systems

When this is done, it will be time for your business – either independently or with a Qualified Security Assessor (QSA) – to carry out the on-site audit, or complete the Self-Assessment Questionnaire (SAQ) (depending on your business' PCI level).

The QSA will discuss the outcome of the audit or SAQ with your organisation, and certify your achievement of compliance if the audit has been successful.

You should then confirm to Worldpay that you have achieved compliance. We will, in turn, report your status to Visa and any other payment card systems where this is required.

As well as protecting yourself against many associated business risks, you will be able to confirm your compliance in your own messaging and marketing collaterals.

3.4 Staying compliant

By achieving compliance you should be providing an acceptable level of protection from the Card Schemes' perspective but it is equally important to ensure that this degree of protection is maintained long-term. PCI DSS compliance is about understanding your risks and meeting the requirements of the standard to ensure you are protected.

To remain compliant, you will need to complete an on-site audit every year, and a Vulnerability Scan every quarter.

We also recommend that you put business processes in place to maintain compliance, including:

- Reviewing your access control policy regularly
- Integrating Vulnerability Scans into your regular business routine
- Ensuring that any new systems or applications are fully compliant
- Creating procedures to make sure your anti-virus systems are regularly updated

You should also ensure that your service providers continue to be PCI DSS compliant. One way to do this is to incorporate relevant clauses into your contracts with them.

© Worldpay 2015. All rights reserved

3.5 General security information

- You must not store Sensitive Authentication Data (SAD) after authorisation even if it is encrypted. This includes full magnetic stripe data, three- or four-digit security codes and PIN/PIN block information (this is the information relevant to the card and the cardholder contained within the chip). If you do not need the data, do not store it.
- You must not use card and verification details for any purpose other than completing the card transaction.
- You must not pass this information to anyone else, except for the purpose of helping you to complete the card transaction.
- You are only allowed to keep a separate record of the card number and expiry date, if both these conditions apply:
    - You have the specific agreement of the cardholder, and
    - You are only going to use this information to help with future transactions, such as recurring payments or new orders believing further orders are likely.
- You must give Worldpay current progress updates about your own PCI compliance when asked, so we can update the Card Schemes. Failure to supply this information could lead to receiving Card Scheme-imposed fines for non-compliance.

© Worldpay 2015. All rights reserved

4 Card Present Transactions

These are face-to-face transactions where your customer and their card are with you at the point of sale.

4.1 Chip and PIN and Contactless

Chip and PIN and Contactless are the usual ways to accept card payments on your terminal when the card and cardholder are present. Some cardholders, however, will continue to sign to authorise payments and this could be due to an impairment that prevents them from inputting their PIN or because their card does not support Chip & PIN technology. Some cardholders will still have magnetic stripe only cards and these must not be refused at the point of sale. Find out more below in Section 4.2

Before you start

- Are you sure that the card belongs to the person presenting it? If you are unsure, call the Authorisation Centre (number detailed in Section 1.5.1) and say that "This is a 'Code 10' call". Find out more about Reducing Fraud in Section 133.

4.1.1 A step-by-step guide (Chip and PIN)

- Following the terminal prompts, key in the full amount of the transaction.
- Ask the cardholder to either insert their card into the chip reader slot on your terminal or separate PIN entry device
- Find out more about how to take a Purchase With Cash Back transaction, if you offer this service. See section 6
- Your terminal will now usually ask the cardholder to enter their PIN. If it doesn't, this could be because the cardholder has a card that does not support chip and PIN technology (such as a chip-and-signature or magnetic-stripe-and-signature card). Your terminal will advise which method is required – always follow the prompts on the terminal
- Ask the cardholder to check that the transaction amount is correct and to enter their PIN.
- Most terminals will then authorise the transaction automatically. If the terminal prompts you, call our Authorisation Centre immediately (number detailed in Section 1.5.1) and follow the instructions. To find out more about Authorisation and referrals see section 5
- Wait for the terminal to print out a terminal receipt.
- Only give the cardholder the goods they are buying when you have received authorisation and completed the transaction. If authorisation is not given, **do not** go ahead with the transaction. Ask your customer for an alternative payment method.
- Ask the cardholder to take their card from the terminal and give them their copy of the terminal receipt.

Keep your copy of all terminal receipts in a secure fireproof place for at least 13 months in case there is a query later or these details are required to help defend a chargeback. Do not alter them in any way. If there is a dispute, the cardholder's copy will normally be taken as correct.

Remember that even where authorisation is given, this is no guarantee of payment and the transaction is still open to being charged back.

4.1.2 A step-by-step guide (Contactless)

Contactless is an increasingly popular method of payment. Contactless cards enable purchases to be completed by tapping the card over a Contactless reader on the enabled terminal. This improves the customer payment experience, speeds up transactions and helps retailers to remove cash from their business.

© Worldpay 2015. All rights reserved

Contactless technology is continuing to evolve and there are an increasing number of consumer Contactless devices such as mobile phones, wristbands and key fobs. These work in the same way as a card, the contactless payment is made by waving the Contactless consumer device over a contactless enabled terminal.

If a card has the following symbol it can be used for contactless payments:

To provide additional security and protect both consumers and retailers the Contactless transaction will occasionally be disallowed and a prompt for a chip and PIN transaction will be made. This is a normal action which has been built into the system.

Please note that the Contactless option is only available where the terminal has been activated for contactless. If your terminal has not been activated, please contact Worldpay and we will be happy to advise how you can offer Contactless payments to your customers.

- Key the full amount of the transaction into the terminal. Note: Purchase With Cash Back is not available on Contactless
- If the total value of the transaction is less than £20 **(NOTE: the UK contactless limit will increase to £30 with effect from 1 September 2015)**/ €15, the terminal will prompt for either a card to be inserted, or tapped against the Contactless reader*.
- Ask the cardholder to check the amount. If cardholder has a Contactless card (check for Contactless symbol – see above), the cardholder will be able to tap the card against the Contactless reader. A PIN is not required to be entered when a Contactless transaction is made.
- Most terminals will authorise the transaction automatically
- Wait for the terminal to print out a receipt, if requested by the cardholder.
- Only provide the cardholder with the goods, or services they are purchasing when you have received authorisation and completed the transaction.

*Whilst the UK contactless limit is increasing to £30, High Value Contactless has already launched. This allows consumers to tap and pay with their smartphones for any value just by using on-device verification (e.g. security code/PIN, fingerprint recognition, etc.) on their handset. For High Value Contactless transactions follow the prompt on your terminal and ask the cardholder to follow the prompts on their smartphone.

For more details on Contactless please see our Contactless Made Easy guide

4.2 When a signature is needed

You should only use a signature to verify a transaction when prompted by your terminal.

In addition, when processing a refund, you (rather than the cardholder) will be required to sign the receipt and the transaction will not require the input of the PIN.

4.2.1 Extra security checks

If you do carry out a transaction using a signature as verification, you should take extra security precautions. Here are some basic ones:

- Make sure the card is not damaged, cut or defaced in any way.
- Check the signature strip for signs of damage or tampering.
- Check any specific security features for that card. Find out more in the Card Recognition Guide. See section 17
- If you are unsure make a 'Code 10' call.

© Worldpay 2015. All rights reserved

Find out more about Reducing Fraud in Section 13.

4.2.2 A step-by-step guide (when a signature is needed)

- Following the terminal prompt, key in the full amount of the transaction.
- Insert the card and follow the terminal prompts which will tell you when a signature is required.
- Most terminals will then authorise the transaction automatically. If the terminal prompts you to, call the Authorisation Centre (number detailed in Section 1.5.1) immediately and follow the instructions. To find out more about Authorisation and referrals see section 5.
- Wait for the terminal to print out a terminal receipt.
- Check that the card number, expiry date and card type on the terminal receipt are the same as on the card. If any details are different, hold onto the card and cancel the transaction immediately. Then call the Authorisation Centre (number detailed in Section 1.5.1) and say that "This is a 'Code 10' call".
- If all the details match, check the transaction and amount, then ask the customer to sign the terminal receipt.
- Check that the signature matches that on the card. If you are not sure, you may decide to ask for additional identification such as a driving licence or a passport. If you are still in doubt call the Authorisation Centre.
- If you are happy with the signature, confirm the transaction on the terminal and give your customer their card and receipt.
- Only give the cardholder the goods they are buying when you have received authorisation and completed the card transaction. If authorisation is not given **do not** go ahead with the transaction. Ask your customer for an alternative payment method. Find out more about Reducing Fraud in Section 133.

See Keeping Records section 2.7, for details of how receipts, paper vouchers and other high security items must be securely stored.

Remember that even where authorisation is given, this is no guarantee of payment and the transaction is still open to being charged back.

4.3 Troubleshooting

You must always follow the prompts on your terminal and **never** magnetic-swipe the card or PAN-key the card number into your terminal to avoid using the higher-level security features (such as chip and PIN).

4.3.1 If the cardholder enters their PIN incorrectly

The cardholder will usually have three chances to enter their PIN. If all these fail follow the prompts on the terminal which will show whether the transaction can be completed on the card or if the cardholder will need to provide another means of payment.

4.3.2 If the cardholder has forgotten their PIN

If your terminal allows PIN bypass follow the terminal instructions. If your terminal does not allow PIN by-pass ask the cardholder for another means of payment.

4.3.3 If you receive a message that the PIN is locked

Please advise the cardholder to get in touch with their card issuer and ask for a new PIN, so that they can start using the card again in the future.

© Worldpay 2015. All rights reserved

4.3.4 If the chip reader does not work

If the card offered contains a chip, the card must be entered into the chip card reader. If a terminal message says the card cannot be read:

Insert the card again (or try again with the card the other way round).

- If this doesn't work the card may be damaged and you can try to swipe the card instead.
- If the card is still unable to be read ask the cardholder for an alternative payment method.

Please note: if you swipe or key enter a chip card and the transaction is later found to be fraudulent, the transaction may be charged back to you.

4.3.5 Failed magnetic stripe transactions – key entry (excluding internationally issued Maestro and Visa Electron cards)

Some customers may have magnetic stripe rather than chip cards. If the terminal says the magnetic stripe cannot be read:

- Try swiping the card again.
- If it still cannot be read, you will be able to key in the card details using the number keys on the terminal.
- Follow the prompts on your terminal which will prompt you for the information needed including the Primary Account Number (PAN).
- After you have entered the PAN and are waiting for authorisation, **you must** use a manual imprinter to obtain an imprint of the card on a paper voucher and complete all details on the voucher. **Do not manually key in the card details to complete a transaction unless you are also able to take an imprint of the card**. The imprint of the card on the paper voucher proves that the card was present when the transaction took place. You may be asked to produce the imprint if the transaction is subsequently queried or disputed.
- Clearly write "no value, swipe failure" on the paper voucher
- The cardholder must sign both the paper voucher and the cardholder receipt printed by the terminal**. Do not send this voucher to us for processing** as the transaction is being completed via the terminal. In the event of a customer query or dispute we will contact you to request a copy of the paper voucher and the electronic receipt.
- Explain to the cardholder why this process is taking place and reassure them that the paper voucher will not be processed but will be held as a record which will be sent to Worldpay if the transaction is disputed
- Check the cardholder's signature matches the one on the reverse of the card.

Please note: if you swipe or key enter a chip card and the transaction is later found to be fraudulent, the transaction may be charged back to you.

4.3.6 If your terminal breaks down completely

If your terminal has stopped working and you have purchased a backup pack, you can still accept card payments using your paper vouchers and imprinter. Find out more in the Terminal Failure section. See section 8

4.4 American Express

Please use the separate instructions provided by this company.

© Worldpay 2015. All rights reserved

5 Authorisation And Referrals

Authorisation and referrals are ways of checking that at the time of taking the transaction the card has not been reported lost or stolen and that there is enough money in the account to cover the purchase. **It's important to understand that authorisation does not guarantee payment.**

5.1 Making a referral call

In the majority of cases, if you have an electronic terminal, the authorisation check is automatic. Sometimes your terminal will prompt you to make a manual authorisation call, known as a referral.

If you have a mobile or portable terminal, this will have been handed to the customer to input their PIN. **You must always take back the terminal from your customer as soon as the PIN is entered. That way you will know whether the transaction has been authorised or whether a referral call needs to be made.**

You must make this call at the time of transaction, while the cardholder is present, and you are holding the card. **Do not hand the card back to the customer until you have received authorisation and the code has been accurately keyed into your terminal.**

See section 1.5 for Authorisation contact numbers

5.1.1 Security questions

During some calls, the cardholder may need to answer one or more personal security questions. Explain that this is part of the card issuer's standard security procedure. The Authorisation Centre will usually ask to speak to the cardholder directly. Once your customer has answered the questions, they should pass the phone back to you. You should not use any information which is given to you by the cardholder. **Only the Authorisation Centre can give you an authorisation code**. You must **not** accept an authorisation code from anyone else (especially your customer).

5.1.2 If the transaction is authorised

You will be given an authorisation code which should be keyed into your terminal when you are prompted. There's more information in your Terminal User Guide about keying the code.

5.1.3 If you are processing on paper

Write the authorisation code clearly on the voucher in the space provided.

5.1.4 If the transaction is declined

- Explain that the transaction has not been authorised and give the card back to the customer, unless the Authorisation Centre asks you to retain it and it is safe to do so.
- If your customer asks why, advise them to contact their card issuer – there is normally a helpline number on the back of the card.
- Remember, transactions are declined for many reasons – it may not be your customer's fault.
- Make sure you destroy any partially completed sales vouchers in front of your customer.
- If your customer still wants to go ahead with the purchase, ask them for an alternative payment method. Remember to check any new card carefully. Find out about Reducing Fraud in Section 133.

© Worldpay 2015. All rights reserved

5.2 Suspicious transactions

If you are suspicious about a transaction, follow the procedures to make a Code 10 call detailed in Reducing Fraud, section 13.

5.3 Transaction changes after authorisation and before processing

Sometimes, you need to make changes to a transaction after you have obtained authorisation. For example, if your customer decides to buy something different, or not to go ahead at all.

If you process payments electronically, you can cancel the sale on your terminal and it will make the adjustments automatically, but this may take a few days to appear on the cardholder's statement.

If you have used a paper voucher for the transaction, cancel it by writing "CANCELLED" across all copies. Then print new vouchers and call the Authorisation Centre again with the following information:

- Card number – 12 to 19 digits across the centre of the card
- Card expiry date
- **Your Customer Number**
- The **Authorisation number you obtained for the original transaction**
- **The original transaction amount** – including any amount of cash back
- **The new transaction amount** – if it is completely cancelled, just say that it is cancelled

A refund would only need to be processed in the event that the transaction has actually been processed. Find out more in Refunds, see section 6.

5.4 Split transactions

You must not split the sale into two (or more) separate amounts on one card in order to avoid obtaining authorisation for the full amount. If a sale is split in this way you may be at increased risk or receiving a chargeback for which you will be liable.

© Worldpay 2015. All rights reserved

6 Refunds

When you make a refund on a card transaction, the amount of the refund is returned to the customer's card account and a corresponding debit will be made to your nominated bank account. If the refund facility is used where there is no corresponding originating transaction, this is not a Refund within the meaning of your contract and this is a breach of your contract for which you will be responsible.

6.1 Before making a refund

Never make a refund unless there was an original purchase. If you do, we may withdraw your card processing facility. We may also suspend or withhold some or all funds for the transactions processed through the facility.

- Check that your customer has given you the card used for the original transaction – **We recommend that the refund is made back to the card used for the original purchase where it is still available. If however such card is not available at the time of refund then you may, at your discretion, use alternate means to issue such refund (in line with your company refund policy).**
- Never give a cash or cheque refund for a card transaction – fraudsters often try to obtain cash this way. **Never refund more than the original transaction amount.**
- If the customer has received a replacement card, the card number may have changed. In this case, take reasonable steps to make sure you refund to the original account. For example, check that the start date of the new card is after the purchase date, and ask them for proof of identity.
- If the card has expired, you should still make the refund back to it, letting your customer know that they need to contact their card issuer to arrange for the funds to be received.

Please note: you could be at risk of a chargeback if a refund is not made to the original card used for the purchase.

6.2 Making a refund using your terminal

The way you do this depends on which terminal you have – please refer to your Terminal User Guide. If you need to use a supervisor card, please make sure that this is kept in a controlled environment and stored securely at close of business each day. If your terminal uses a supervisor code you should ensure it has been personalised (i.e. changed from any default setting to prevent it being guessed by potential fraudsters), and only known by those people you have authorised to make refunds. It is your responsibility to ensure that you keep your supervisor code or supervisor card safe and secure and you will be responsible and liable for any improper use of the refund facility by your employees or others.

Once you have processed the refund, an authorised person needs to sign the receipt. Your signature confirms you have given permission for the funds to be transferred from your bank account back onto your customer's card.

6.3 Making a refund using paper vouchers and the manual imprinter

- Use a red Worldpay refund voucher, marked REFUND.
- Put the customer's card in the imprinter, with the refund voucher on top, and print as usual.
- Give the card back.
- Write on the voucher what the refund was for.
- **Sign the voucher yourself.**
- For the refund to reach the customer's account, **you will need to post the refund voucher to us within three working days.** The address to post these to is:

  VPU
  Worldpay

© Worldpay 2015. All rights reserved

Victory House
5th Avenue
Gateshead
NE11 0EL

- Please see section 8 for further details relating to the use of paper vouchers

See Keeping Records, section 2.7, for details of how receipts, paper vouchers and other high security items must be securely stored.

6.4 American Express refunds

Please use the separate instructions provided by this company.

© Worldpay 2015. All rights reserved

7 Purchase With Cash Back

Purchase With Cash Back (PWCB) may be good for your business and the people who shop with you. For your customers, being able to get cash when they spend at a local outlet is a convenient way to save time. That could encourage them to visit more regularly – potentially boosting your takings. From a security perspective, PWCB also reduces the amount of cash held on the premises, making your business less vulnerable to crime.

7.1 To offer Purchase With Cash Back:

- You will need Worldpay's agreement to offer Purchase With Cash Back.
- You must process the transaction through your terminal. If your terminal is not working, you cannot offer cash back (i.e. you cannot use paper vouchers for this).
- Your customer must be making a purchase at the same time as requesting cash back.
- Your customer must be present to enter their PIN (or sign the terminal receipt if the card does not support chip and PIN).
- The amount of cash back must not be more than £100 for UK customers and €100 for those in ROI.
- Your customer must use one of these cards:
  - Maestro
  - Visa Debit
  - Visa Electron
  - European-issued Debit MasterCard

7.2 Before you start

- Be sure that the card belongs to the person presenting it. If you are suspicious you could ask the cardholder for other identification such as a driving licence or a passport. Find out more in Reducing Fraud. See Section 13.
- The PWCB process is not the same for all terminals. As well as following the basic step-by-step guide below, read your Terminal User Guide for specific instructions.
- If you are suspicious about the card or the cardholder, call the Authorisation Centre (number detailed in Section 1.5.1) and say, "This is a 'Code 10' call". The operator will talk you through the process.

7.3 A step-by-step guide

- Ask the cardholder to insert their card into the chip reader slot on your terminal or separate PIN entry device.
- Following the terminal prompts, key in the full amount of the transaction, then enter the PWCB amount separately.
- Your terminal will advise which method is required - always follow the prompts on the terminal.
- Your terminal will now usually ask the cardholder for a PIN. If it doesn't, this may be because the cardholder has a non-UK-issued card, or an impairment that means they need to sign. For non-chip and PIN transactions, you should check that the card is not damaged and shows no sign of having been cut or written over. You should also check the specific security features for the card you are accepting. Ask the cardholder to check that the transaction amount is correct and enter their PIN.
- Most terminals will then authorise the transaction automatically. If the terminal prompts you to call the Authorisation Centre then you must do so immediately (number detailed in Section 1.5.1) and follow the instructions.
- Only give the cardholder the goods they are buying and the cash amount when you have received authorisation and completed the card transaction. If authorisation is not given, **do not** go ahead with the transaction. Ask your customer for an alternative payment method.
- Wait for the terminal to print out a terminal receipt.

© Worldpay 2015. All rights reserved

- Confirm the transaction on the terminal and give your customer the goods they have purchased, the cash amount, their card (they should remove it from the PIN pad if a chip and PIN transaction) and their copy of the terminal receipt.

  See Keeping Records, section 2.7, for details of how receipts, paper vouchers and other high security items must be securely stored.

© Worldpay 2015. All rights reserved

8 Terminal Failure

You should always use your electronic terminal to process card transactions. If your terminal stops working temporarily because of a fault, or if your power supply or telephone connection is interrupted, you can use our 'back-up' service, of card imprinter and paper vouchers only, until the terminal is working again.

8.1 Using paper vouchers

You must only use paper vouchers as a 'back-up' when your terminal is not working or if your terminal instructs you to do so. You should advise Worldpay or your terminal supplier as soon as possible if your terminal is not working.

While you are using paper vouchers, you can only take Debit MasterCard, MasterCard Credit, Visa Credit, Visa Debit, JCB or Diners/Discover payments. You will not be able to accept Visa Electron, Maestro or any card that doesn't have raised numbers.

Remember you can only accept card types listed in your Contract. If you take any others, the transaction may be returned unpaid.

You need to call for authorisation for every transaction using paper vouchers. Find out more in Authorisation and Referrals. See section 5

Never split a transaction into two or more separate amounts on the same card, or split a transaction between two or more different cards or vouchers as a way of avoiding authorisation or referral of the full amount on one card. You can split transactions between a card payment and cash though. For the card element you will need to telephone for authorisation.

8.1.1 American Express

Please use the separate instructions provided by this card company.

8.2 Before you start

Before you start using paper vouchers for transactions featuring any of the card types mentioned in the previous section follow the steps below. You should also carefully follow guidance in Reducing Fraud, See Section 13 as paper vouchers carry a higher risk of fraud than if payment is made by Chip and PIN.

- Make sure that the card is not damaged and shows no signs of having been cut or written over. You should also check the specific security features for the card you are accepting. Find out more in our Card Recognition Guide. See section 16.
- Only use Worldpay vouchers.

8.3 A step-by-step guide

- Place the imprinter on a firm surface, with its sliding bar all the way over to the left.
- Put the card into the imprinter with the raised numbers facing upwards. Make sure the card is securely slotted into the right place or you might damage it.
- Place the Worldpay voucher on top of the card and tuck it in.
- Slide the bar from left to right and then back again. You don't need to press down or force it.
- Take the voucher out and check the numbers have printed through clearly on each sheet. If they haven't, destroy the voucher and try again with a new one.

© Worldpay 2015. All rights reserved

- If you cannot get a good imprint **do not write the card details on over the top**. If you keep having problems with the imprinter, contact the Worldpay Helpdesk immediately to order a replacement and ask how to proceed.
- When you have a good imprint, complete the voucher by writing the full details of the transaction clearly in the appropriate sections of the voucher with a ballpoint pen. Complete the amount in both pounds and pence.
- Ask your customer to check and sign the voucher, while you hold the card and watch them sign.
- **Check that the signature on the voucher matches the one on the card.**
  You should always call for authorisation when using paper vouchers. If you are suspicious, when you call the Authorisation Centre (number detailed in Section 1.5.1) say, "This is a 'Code 10' call"
- Only give the cardholder the goods they are buying when you have received authorisation and have completed the transaction.
- If you are given an authorisation code, write it clearly on the voucher in the space provided using a ball point pen.
- If authorisation is not given **do not** go ahead with the transaction. Destroy the partially completed voucher immediately. Ask your customer if they can pay with another card or cash. If you are offered another card for payment you must also obtain authorisation on the new card before starting a new transaction.
- When the transaction is complete, give the card back to the cardholder together with the top copy of the voucher and the goods they have purchased.
- Keep the rest of the voucher copies for processing and for your records.

See Keeping Records, section 2.7, for details of how receipts, paper vouchers and other high security items must be securely stored.

8.4 Making a refund using paper vouchers

- Use a red Worldpay refund voucher, marked REFUND.
- Put the customer's card in the imprinter, with the Worldpay refund voucher on top, and print as usual.
- Give the card back to the cardholder.
- Write on the voucher what the refund was for.
- **Sign the voucher yourself.**
- For the refund to reach the customer's account, you will need to send us the refund voucher within three working days. Details of the address to post these to are in section 8.5 below

8.5 Processing paper vouchers

For the money from paper voucher transactions to reach your bank account, you need to complete and send us a Banking Summary Voucher.

If you have made any refunds using paper vouchers, you will also need to send to us the processing copy of the refund vouchers.

The address to send these to is:

VPU
Worldpay
Gateshead Card Centre
5th Avenue
Gateshead
NE11 0EL
United Kingdom

© Worldpay 2015. All rights reserved

The Banking Summary Voucher has three parts:

- **White** – processing copy
- **Blue** – this copy is for your records.
- **Yellow** – this copy is also for your records.

8.5.1 How to prepare Banking Summary Vouchers

- Place your Banking Summary Card in the imprinter together with the Banking Summary Voucher and take an imprint of your retailer card.
- Turn the voucher over and complete the back of the white copy:
  - List the individual amounts of the sales vouchers
  - Calculate and complete the total of all sales vouchers.
- Turn the voucher back over so that the blue copy appears and write in:
  - The number of sales vouchers and their total value
  - The number of refund vouchers and their total value
  - The total amount by deducting the refunds from the sales. If the value of the refund vouchers is higher than sales, then put a minus sign in front of the total to show it is a negative value
- Sign and detach the white copy and put it with the sales vouchers, in the same order they are listed, plus any adding-machine listing(s) if you have used these.
  - Please do not use staples, pins or clips to hold the vouchers together.
- Keep the blue and yellow copies for your records and to help you when you reconcile your bank statement.
- Please send the white copies of the Banking Summary Voucher and paper voucher(s) within three working days to the Voucher Processing Unit at:

  VPU
  Worldpay
  Gateshead Card Centre
  5th Avenue
  Gateshead
  NE11 0EL
  United Kingdom

The maximum number of vouchers you can submit with a Banking Summary Voucher is 200, but you can submit more than one Banking Summary Voucher at a time. If your list of transactions won't fit on the back of the Banking Summary Voucher, please include a separate list of the amounts making up the total. This could be an adding-machine listing.

8.5.2 Adjustments

- If there are any errors on the Banking Summary Voucher, we will write to you with full details. Any adjustments are normally made to your account within five working days of the date of the letter.
- Any adjustment will be made to the account from which we normally debit your service charge, unless you have made different arrangements with us.

© Worldpay 2015. All rights reserved

9 Card Not Present Transactions

Card not present (CNP) transactions are those where the card and cardholder are not with you at the point of sale. Offering your customers this option gives you and them extra flexibility, but it's important to understand that you will need Worldpay's agreement to accept these transactions:

- Mail Order Telephone Order Transactions
- eCommerce Transactions

CNP transactions also carry a higher risk of fraud so please carefully read the Reducing Fraud section covering CNP transactions. See section 13.4.

9.1 Can I accept CNP transactions?

Before deciding to accept CNP transactions you should consider all risks to your business, because they carry a higher risk of fraud and you will be financially liable if a transaction is confirmed as invalid or fraudulent.

You can only accept CNP transactions if the CNP section of your application (which forms part of your Contract with us) has been completed and accepted by us. If it has not, and you would like to make CNP sales, please contact the Worldpay Helpdesk.

Having Worldpay's agreement to accept CNP transactions does not automatically allow you to accept card payments over the Internet. To do this, you will need to have an agreement with Worldpay that allows you to accept eCommerce payments and an Internet payment facility. To find out more, please read more in eCommerce transactions.

9.2 Authorisation

All CNP transactions must be authorised.

Authorisation is not a guarantee of payment –Authorisation simply means that at the time the transaction was taken and you obtained authorisation the card has not been reported lost or stolen and there are sufficient funds available. *Authorisation cannot always validate the address you have been given and therefore you should consider undertaking additional checks as appropriate.*

The authorisation number for CNP transactions is detailed in Section 1.5.2.

Find out more about Authorisation And Referrals in Section 5.

© Worldpay 2015. All rights reserved

10 Mail Order And Telephone Order

This section covers only Mail Order and Telephone Order (MOTO) sales. Find out more about taking card payments over the Internet in eCommerce sales.

10.1 Which cards can I accept?

You can accept:

- MasterCard
- Debit MasterCard
- Visa
- Visa Debit
- Visa Electron
- Domestically issued Maestro
- JCB
- Diners/Discover

10.2 Reduce the risk of fraud

Most MOTO sales are genuine. However, because they are relatively anonymous – you don't see the card or the shopper – some people see it as a less risky way to attempt fraud. Many want to obtain goods they can sell on for cash; others 'card test', placing an order to check if the card details they have will be authorised.

If a MOTO transaction is disputed, it is very difficult to prove that the real cardholder ordered the goods. To reduce the risk of fraud and financial loss to your business, it is extremely important to follow the correct procedures.

Find out more about Reducing Fraud in section 13 and Additional security checks for MOTO transactions in Card Not Present Transactions (CNP) See section 13.4.

10.3 What details do I need from the cardholder?

To process a MOTO transaction, you will need to take the cardholder's:

- Card number – the long number across the centre of the card
- Name as it appears on the card – including any initials
- Card expiry date
- Full postal/billing address, including postcode, as it appears on the cardholder's statement
- Chosen delivery address – if different from above
- Card Security Code (CSC) - three-digit code at the end of the signature strip (**NOTE** – CSC needed for telephone order transactions only, NOT required for Mail Order transactions)

If you have a limited returns policy, such as no refunds, you must make this clear to customers before asking for payment. To avoid disputes, we recommend you ask them to agree to your terms, in writing if possible, before completing the transaction.

Never ask for a customer's PIN.

© Worldpay 2015. All rights reserved

10.4 The Data Protection Act 1998

Please remember that if you are collecting personal data like the above, you need to register as a data controller and comply with your obligations under data protection legislation. Worldpay will not take responsibility if you fail to do this and action is taken against you.

10.5 How to complete a MOTO transaction

Follow the prompts on your terminal and enter the information asked for, including the additional security checks of the Card Security Code and Address Verification Service if your terminal is set up for these services. The exact process depends on the terminal you have. Please read your Terminal User Guide to find out more.

10.6 Additional security checks for MOTO transactions

To help make MOTO transactions as secure as possible, you will need to key in details on your terminal for both of the following. You will then get a response on your terminal to help you decide whether to go ahead with the sale.

10.6.1 Card Security Code (CSC)

This is a three-digit code at the end of the signature strip or in a separate white box next to the signature strip. American Express cards have a four-digit CSC on the front of the card. (NOTE – CSC needed for telephone order transactions only, NOT required for Mail Order transactions). **Never record the CSC – it must only be used for one transaction.**

10.6.2 Address Verification Service (AVS)

NOTE: The 24 x 7 Worldpay Helpdesk can carry out a name and address check over the telephone. This service verifies that the name and address details provided match the details registered to the card issuer. A fee applies to this service. Contact the Name & Address Check team for details. See section 1.5.3 for contact details

AVS is also available via Worldpay terminals and can be used to check the numerical part of the cardholder's registered billing address with the card issuer. Care should be taken when obtaining details from the cardholder to ensure the address detail provided are exactly those they have registered with their card Issuer (i.e. as it will appear on their statement) to avoid a possible address mis-match.

Due to the nature of overseas addresses and the way in which they are stored by card issuers, we may not, in all cases, be able to provide a full address match.

Examples of CSC and Address Numbers

- Card number - 5123 4567 8901 2345
- Three-digit CSC – 696

Mr AN Other
22 High Street
Anytown
AB**1 2**BB

You should key...
CSC: 696
Postcode numbers: 12
Address number: 22

Mr A N Other
Flat **4**
22 High Street
Anytown
AB**1 2**BB

You should key...
CSC: 696
Postcode numbers: 12
Address number: 422

© Worldpay 2015. All rights reserved

Mr AN Other
Level **10**
Tower Building
200 High Road
Anytown
AB**1 2**BB

You should key...
CSC: 696
Postcode numbers: 12
Address number: 10200

12345 Corporal A N Other
BFPO **7899**
22 Sun Avenue
Cyprus
CYP **12**

You should key...
CSC: 696
Postcode numbers: For BFPO addresses no data is to be entered in this field.
Address number: 78992212* (the first eight numeric starting with the BFPO number)

Mr AN Other
Home Farm Cottage
Lane End
High Village
Anytown
LU**3 1**NH

You should key...
CSC: 696
Postcode numbers: 31
Address number: If no numbers just press **Enter**.

Mr AN Other
22 Wall Street
New York
1234567*

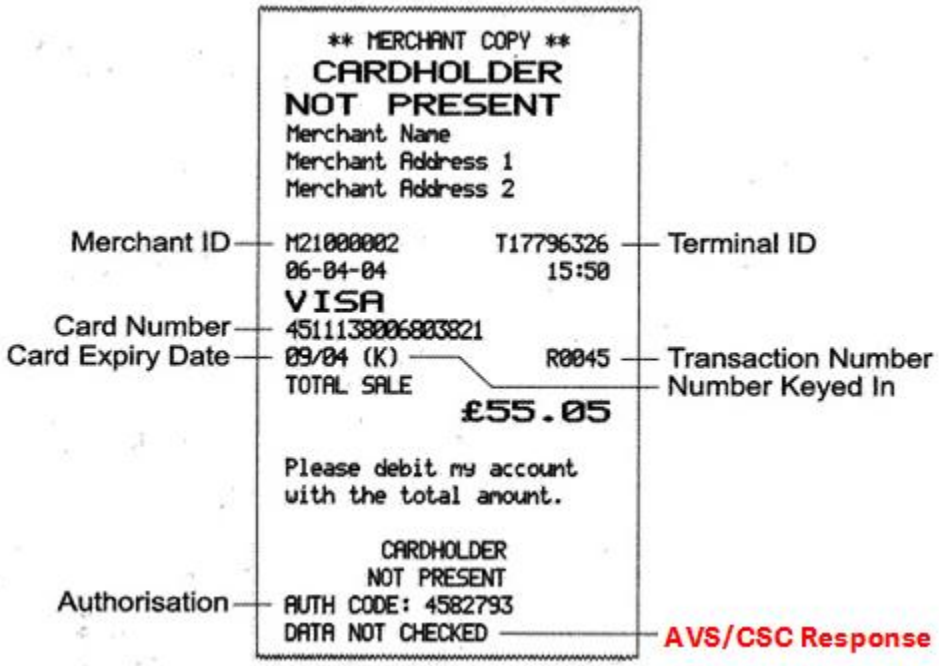
You should key...
CSC: 696
Postcode numbers: (first eight numerics of ZIP code)
Address number: 22

**Some terminals may limit the number of digits which can be entered in these fields. Where this is the case enter as many digits as your terminal will allow.*

What do the CSC/AVS responses mean?

After you have keyed in the CSC and AVS data, as long as the transaction has been authorised, one of the responses shown below will appear on your terminal. It can also be found at the bottom of your copy of the till receipt. Please read the response carefully, as in some cases it will identify a higher risk i.e. if data cannot be matched.

© Worldpay 2015. All rights reserved



It's important to understand that these checks are an additional security measure and can help you make an informed decision, but they are not a guarantee of payment.

The below tables shows CSC/AVS responses however it is important to note that the exact wording of the response may vary depending on the terminal or service provider you use. Please refer to your terminal or service provider if a different response is received. Having carried out these checks, it is your responsibility to understand what the response means and to decide whether you want to proceed with the transaction.

Response	What this means	What we suggest you do
Data Matched	Both the CSC and AVS match the card issuer's records.	If you have been given an authorisation code and there are no other suspicious circumstances, in most cases you will want to go ahead with the sale, as long as you are confident you can securely deliver goods/services to the address that has been verified. Delivering to a different address increases the risk associated with any CNP sale. Find out more in Reducing Fraud.
Card Security Code Matched	The CSC matches. Address postcode and house number details cannot be fully matched.	There is a possibility that the transaction is fraudulent, but it could also mean that the cardholder has moved recently and not updated their details with their card issuer. Another possibility is that the details have been taken down incorrectly or that the cardholder address is abroad and we have been unable to verify with the card issuer. Before going ahead, you should check the address details with your customer and satisfy yourself that they are the rightful cardholder before progressing with the sale.
Address Match Only	CSC cannot be matched. Address postcode and house number details match.	There is a possibility that the transaction is fraudulent, but it could also mean that the cardholder has given you the wrong CSC. Before going ahead, check the CSC with the customer and satisfy yourself that they are the rightful cardholder. **Beware** of repeated attempts by the cardholder to get the CSC right. This could indicate fraud. Please read the Reducing Fraud

© Worldpay 2015. All rights reserved

		guidance in section 13.4
Data not Matched	The CSC and one or both of the address number details do not match.	There is a possibility that the transaction is fraudulent. We recommend you do not go ahead without further checks to satisfy yourself that the person offering the card is the rightful cardholder. For example, you should ask for additional ID, such as a copy of the passport or driver's licence, or ask for copies of utility bills.
Data not Checked	The card issuer has not been able to check the data.	This could be because the card issuer doesn't support either of these security checks or their system is down. If this happens you need to make a decision based on the information you have, to satisfy yourself that the person offering the card is the rightful cardholder, before processing the transaction.

10.7 Making an informed decision

Even when the AVS and CSC do not match, the transaction may still be authorised for the value of the transaction. If this happens, it is your decision whether to accept or decline the transaction based on the results of the CSC/AVS checks. **Please remember that these checks are not a guarantee of payment.**

It's up to you to decide whether to proceed or not. **When you make your decision, bear in mind that you will be financially liable if the transaction is confirmed as invalid or fraudulent/returned unpaid by the card issuer, even if the CSC/AVS data matches and an authorisation code has been given.**

10.8 Protect your business

Most MOTO sales are genuine but the risk of fraud is higher because the cardholder and card are not present. Follow all the processes outlined in this section and refer to Reducing Fraud. See section 13

These additional checks via your terminal cannot confirm cardholder names and therefore you should take additional steps to do so if you are in any way unsure about the transaction.

10.9 Delivery, documents and record-keeping

Goods ordered by mail or telephone order must be delivered to the person who ordered them and not released to third parties, including relatives, couriers not arranged by your business and taxi drivers.

A signature should be obtained from the cardholder as proof of delivery – this can be used as evidence in the event that a dispute subsequently arises.

For all MOTO transactions you must send the following documents to the cardholder with the delivery:

- Sales invoice, to support the transaction
- Cardholder's copy of the receipt from the terminal

See Keeping Records, section 2.7, for details of how receipts, paper vouchers and other high security items must be securely stored

If a cardholder wishes to collect the goods they must come to your premises in person and produce their card. In this case, **you must either cancel or refund any previously-completed MOTO transaction and process a new card present transaction**, following the instructions in your terminal guide and the prompts on your terminal.

© Worldpay 2015. All rights reserved

11 eCommerce Transactions

We provide a range of services to enable you to trade online. Our gateway solutions are designed to simply connect to your eCommerce store.

11.1 Important

- Before you can make eCommerce sales, you need an agreement with Worldpay that allows you to accept Ecommerce transactions.
- When this arrangement is in place we will give you guidance about setting up and integrating your website with our gateway.
- You will need a specific eCommerce customer account.
- You will be issued with a new customer account just for your eCommerce sales. You must never use an existing non-ecommerce account for your online sales.
- Your floor limit for eCommerce sales will be zero to ensure all transactions are authorised
- You must always advise Worldpay if you intend to take transactions from a new website we had no prior knowledge of.

11.2 Payment types you can accept

Our Gateway solutions allow you to accept a wide range of credit and debit cards, including:

- Visa Debit and Credit
- MasterCard Debit and Credit
- Maestro
- Visa Electron
- American Express
- JCB
- Diners/Discover
- ELV

11.3 Reducing fraud and chargebacks

Most eCommerce sales are genuine. However, because the Internet is relatively anonymous – you don't see the card or the shopper – some people see it as a less risky way to attempt fraud. Fraudsters want to obtain goods they can sell on for cash; others 'card test', placing an order to check if the card details they have will be authorised. See How To Combat ECommerce Fraud, section 13.4.3

If an eCommerce transaction is disputed, it is very difficult to prove that the real cardholder ordered the goods and you will be responsible for any challenge raised. **To reduce the risk of fraud and chargebacks, it is extremely important to follow the correct procedures**.

When making an eCommerce sale, you must do all you can to check your customer's identity and make sure that they are entitled to use the card being offered. If you employ a third-party Payment Service Provider (PSP) to capture and process your eCommerce transactions, they should deal with the below process for you. Note that you should only use a PSP that is compliant with the PCI DSS requirements – see chapter 3, Payment And Information Security.

Details to collect

- Card number

© Worldpay 2015. All rights reserved

- Card expiry date
- Cardholder's name and initials as they appear on the card
- Cardholder's full postal address/billing address
- Delivery address, if different
- Card Security Code (if your PSP software is enabled to capture these details) – the last three numbers on the signature strip (Please note: This information must only be used for one transaction and must not be stored for future use). Example Cards has details of card features including the location of the CSC code, see section 17.3

Authorisation

- The telephone number for authorisation for eCommerce transactions is detailed in Section 1.5.1.
- **Authorisation of a transaction does not guarantee payment.**
- **Authorisation only checks that at the time of the transaction the card has not been reported lost or stolen and the availability of funds. Authorisation cannot always validate the address you have been given and you should consider undertaking additional checks as appropriate.**

Find out more about Authorisation and Referrals. See section 5

11.4 Cancellations after an eCommerce order is taken

- If an eCommerce transaction is cancelled for any reason and the original transaction was authorised, you must let the Authorisation Centre know or refer to your implementation pack for contact details.
- If you employ a third-party Payment Service Provider to capture and process your eCommerce transactions, you must also let them know that the transaction is cancelled.
- If the transaction has already been processed, you will need to make a refund.

11.5 Keeping customer data secure

- Card details must be captured and stored securely, either on your own secure server or by a PSP able to connect to Worldpay.
- Card details must always be encrypted and the host server must be protected by a **firewall.**
- **E-mail is not a secure way to transfer card transaction data. You must ensure that the card number is omitted from the order confirmation message sent to your customer.**
- To find out more about payment and information security visit our SaferPayments website

11.6 Cardholder Authentication

Cardholder Authentication is a security tool designed to help you authenticate cardholder details in the online eCommerce environment. It brings together the 3D secure cardholder authentication schemes that verify a cardholder's identity when they make an online purchase - MasterCard SecureCode, Verified by Visa and American Express SafeKey.

These systems enable an online shopper to prove they are the genuine cardholder by entering a unique password at the shopping-cart stage. . This is an additional check where a security "box" may appear on screen allowing the shopper to enter elements of their unique password. This feature is provided by the shopper's card issuer and will usually appear within your payment page. The process only takes a few seconds and the customer is unlikely to notice any interruption to the sale process.

Most chargebacks happen when a cardholder denies that they have made a purchase. This security tool goes a long way towards proving that a sale is genuine. If you have Cardholder Authentication and offer it to your customers, you will be protected from most chargebacks with a fraudulent reason code.

Please note that the use of MasterCard SecureCode is compulsory for eCommerce Maestro transactions.

 © Worldpay 2015. All rights reserved

11.7 If you change your payment service provider (PSP)

If you decide to change your PSP, please contact the eCommerce Helpdesk with your new details. They will arrange for a new customer number to be set up for you so that you can begin trading with your new PSP as soon as possible.

11.8 Guidance notes

Supplementary requirements for accepting ecommerce transactions

Before you accept any eCommerce sales, you must have an agreement with us to do so. Your attention is specifically drawn to the following:

If you process an ecommerce transaction without having an ecommerce agreement to do so, any authorisation given by us will not mean that we have varied our requirement for an ecommerce agreement. Any eCommerce transaction authorised in this way will be subject to full chargeback rights against you if the transaction is charged back against us for any reason.

Failure to advise Worldpay of your intention to take transactions over the Internet or to advise us of a new website URL we had no prior knowledge of is a breach of your contract and may result in termination of your Contract with Worldpay and/or in fines from the Card Schemes for which you will be responsible.

Before you carry out any ecommerce sales, your legal advisers should review your website to check that all contractual and legal issues are covered adequately and the website contains appropriate disclaimers and restrictions.

As a minimum, your website must clearly display:

11.8.1 Information about your business

- **Who you are** – you must clearly disclose your business name so that cardholders can easily determine who they are dealing with (and distinguish you from other parties such as your suppliers). Your website domain name must be recognisable to the cardholder based on their online shopping experience. If you are a company, you should include your full company name and incorporation/registered number, together with your physical and online addresses. Your identity should be consistently conveyed on all communications with the cardholder.
- **A customer service phone number** (including both country and area codes) that cardholders can use to resolve disputes. The number quoted must not be that of a mobile phone. If you deliver goods or services internationally, both domestic and internationally accessible numbers must be listed. Your e-mail address should allow you to be contacted 'directly and rapidly'. This should be the e-mail address of your customer service desk if you have one.
- **Your VAT registration number.**
- **Details of any Trade Association membership**, including registration number, details of the code of conduct to which you subscribe and details of how to contact them.
- **Details of any professional body you are registered with**, your professional title, the member state which granted it and a reference to the applicable professional rules in that member state and information as to how these rules can be consulted electronically.

11.8.2 Information to be given before an order is placed

- **A description of the products and services** (including any guarantees) you are offering, clearly explaining your shipping practices together with any export restrictions. The cardholder must be able to clearly determine when they can expect to receive their merchandise.
- **Total costs for products or services**, including all appropriate shipping, handling and tax charges. You must quote all prices in a currency agreed with us and the currency offering must be clear to the cardholder. Where applicable, you should indicate details on currency conversion (exchange rate).

© Worldpay 2015. All rights reserved

- **Clear, easy-to-find terms and conditions and procedures**, which state the exact commitment that the cardholder is being asked to make, must be made available in a format that the cardholder can store and reproduce.
- **Your returns policy** must be made clear to the cardholder before payment is requested. If a refund policy is offered, it should include a full refund of the amount of the shipping, handling and applicable tax charges.
- **Your cancellation policy** must be made clear to the cardholder before payment is requested. If you are offering a free trial period, it must specify exact dates that the free trial ends and the consequences of non-cancellation.
- **A clear statement that the cardholder is committing to a payment** where they are prompted to enter their account number, giving an option to cancel at that point. You may only request a card account number as payment for goods or services and must not request or use the account number for age verification or any other purposes other than payment.
- **Clear instructions on how to complete the order** together with instructions for correcting input errors before the order is placed, irrespective of the way the order is taken or may be accessible thereafter.
- **Details of languages** offered for conclusion of the order.

11.8.3 Information to be given after the order is placed

- An effective, accessible way to correct any input errors which took place at the point of confirmation
- An e-mail acknowledging receipt of the order, which must be sent the customer 'without undue delay'
- Confirmation in 'durable form' – such as e-mail – of:
  - The name and geographical address of your business
  - A description of the main characteristics of the goods
  - The price, including all taxes and delivery costs where appropriate
  - Arrangements for payment and delivery
  - The geographical address to which any customer complaint should be addressed
  - Information about after-sales service and guarantees

11.8.4 Commercial communications

You must ensure that any unsolicited commercial communication sent by e-mail is clearly and unambiguously identifiable as soon as it is received. You must clearly identify in all communications, any promotional offer (including any discount, premium, gift or competition) and ensure that any conditions which must be met to qualify for it are easily accessible, and presented clearly. You must also comply with the following basic standards:

- Data Protection Legislation within the applicable law must be adhered to in order that the collection of personal information is not processed, traded or disclosed illegally.
- You must ensure you have appropriate operational and technological processes and procedures in place to safeguard against the unauthorised access or unlawful processing, or disclosure, of personal information. The security measures you must take include the use of the most up to date technologies to protect the personal information collected or stored on your web site and/or systems. Especially sensitive or valuable information, such as financial data, should be protected by reliable encryption technologies.
- Distance-selling requirements must be complied with as laid down in the applicable law[1].
- Complying with other applicable trading standards and laws and regulations as the same are created from time to time.

[1] A Guide for e-Business to the *EC Directive regulations 2002* and related material can be found on the HMSO website www.legislation.hmso.gov.uk

© Worldpay 2015. All rights reserved

12 Recurring Transactions

Recurring transactions are a convenient way for you to collect regular payments, such as membership subscriptions and monthly insurance premiums, from customers. To avoid any disputes, it's very important to ensure that you carry out your customers' instructions properly and make it easy for them to get in touch to change or cancel payments.

12.1 The basics

To set up a recurring transaction, you must:

- Have an agreement with Worldpay that allows you to take recurring transactions.
- Use the Customer Number from this agreement, **not** your normal Customer Number.
- Have the cardholder's written authority.
- Check the card is one of these: MasterCard, Visa Credit, Visa Debit, Visa Electron, JCB, Debit MasterCard, Diners/Discover
- Recurring transactions cannot be completed with a Maestro card.
- Obtain authorisation for the first payment in the recurring transaction string using a secure method:
  - Chip and PIN for card present transactions, or
  - Card Security Code (CSC) for Mail Order Telephone Order (MOTO) transactions, or
  - Verified By Visa/MasterCard SecureCode for eCommerce transactions
- Never process a transaction that is declined.
- Supply a telephone contact number that will appear on the cardholder's statement (and let us know if this number changes).

12.2 Obtaining written authority

You must have a written authority form signed by your customer allowing you to take payments from their card account. This form must show the cardholder's:

- Name
- Full address
- Postcode
- Telephone number
- Card account number
- Card expiry date
- Agreed payment pattern (Find out more in Recurring Transaction options below.)
- Authority and understanding the authority will remain in force until such time as it is cancelled in writing

Never ask for a customer's PIN nor store your cardholder's Card Security Code (CSC). The CSC may be used for the first transaction but is not required for subsequent transactions.

See an example of a written authority in Section 12.5.

The Data Protection Act 1998: Please remember that if you are collecting personal data such as the above, you need to register as a data controller. Your failure to do this and any subsequent action that may be taken against you will not be the responsibility of Worldpay.

See Keeping Records, section 2.7, for details of how receipts, paper vouchers and other high security items must be securely stored.

© Worldpay 2015. All rights reserved

12.3 Recurring transaction options

You have two options for collecting payments:

12.3.1 Option 1 – A fixed amount on a fixed day: no notice needed

- The payment period could be weekly, monthly, three-monthly, six-monthly or yearly.
- The cardholder should agree this on the written authority form.
- When you have this authority, you don't need to let the customer know when you will be taking payments, unless:
  - The amount and/or dates change after the initial agreement – then you must write to the cardholder giving 14 days notice before the first new payment.
  - The payment period is more than a year – then you must write to the cardholder giving 14 days notice before each payment is due.

12.3.2 Option 2 – Variable amounts or days: giving notice

- If the amount to be paid and/or the payment dates are variable, this should be stated on the written authority form.
- You must write to the cardholder giving 14 days notice before collecting each payment, telling them the amount due and the date on which the money will be collected.
- When you have written to let the cardholder know that a payment is due, or about a change in dates/amounts, there is no need for them to respond.

12.4 Cancellation

It's important to understand that a cardholder may cancel their authority to debit their card account at any time.

You must act on their instructions and collect no further payments. If any payment is returned unpaid – for example, if the account has been closed – you must contact the cardholder and ask them to pay in another way. Never re-debit the card as this may lead to chargebacks and ultimately suspension or termination of your Worldpay facility.

12.5 Important information for eCommerce customers

If you offer recurring transactions for eCommerce sales, you must:

- Notify cardholders clearly at the outset that subsequent payments will be taken from their account.
- Offer an online cancellation facility.
- State clearly if you are offering a fee-free period and give the cardholder at least seven days notice of the expiry of any fee-free period.

© Worldpay 2015. All rights reserved

Example – written authority form

Recurring

Transaction authority

Please complete parts 1 to 7 to authorise us to claim payments directly from your Account.

To: Customer & Co. Ltd

Customer Reference

1. Name of Cardholder

2. Full Address

3. Postcode

4. Telephone Number

5. Account number

6. Expiry Date

7. I authorise you to charge my account an unspecified amount in respect of _____ as and when they become due.*

I understand that [insert company name] will advise me of the amount to be paid and the dates on which payment is due and that [insert company name] may only change these after giving me prior notice.

I UNDERSTAND THAT THIS AUTHORITY IN FAVOUR OF [insert company name] WILL REMAIN IN FORCE UNTIL SUCH TIMES AS I CANCEL IT IN WRITING TO [insert company name].

Signature_____

Date_____

** Please insert details of the goods/ services being purchased.*

© Worldpay 2015. All rights reserved

13 Reducing Fraud

Card Present Transactions	Card Not Present Transactions: Mail Order Telephone Order	Card Not Present Transactions: eCommerce
These are face-to-face transactions where your customer and their card are with you at the point of sale.	These are sales made by mail or over the telephone where the customer and their card are not with you at the point of sale.	These are sales over the Internet where the customer and their card are not with you at the point of sale.

Card fraud is becoming increasingly sophisticated and, if you are not vigilant, can result in financial loss for your business. Your exposure to fraud will depend upon how aware you are of the risks and how carefully you and your staff handle card transactions. This section gives you some useful tips to help you reduce your risk of losing money through fraud.

Before deciding to accept CNP transactions you should consider all risks to your business, because they carry a higher risk of fraud and you will be financially liable if a transaction is confirmed as invalid or fraudulent.

13.1 Always remember

- Follow all the prompts on your terminal.
- Be alert and aware – for card present transactions, if you are suspicious about a card or the person presenting it, make a 'Code 10' call and follow the prompts.
- Be discreet when you are suspicious – don't take risks with anyone's safety.
- If your terminal has a supervisor card or code, keep it safe and secure – anyone who has access to this could make fraudulent refunds to a card which may result in financial loss for your business.
- Never allow a third party to authorise or process card transactions using your facility – this would breach your contract with us and may result in withdrawal of your facility and/or in Card Scheme fines. You will be liable for any fraud/chargebacks irrespective of the fact you have processed transactions on behalf of someone else.
- Keep your terminal in sight during a transaction and take it back from your customer as soon as they have entered their PIN.

Authorisation does not guarantee payment. It simply means that at the time of the transaction the card has not been reported lost or stolen and that there are sufficient funds available. Find out more about Authorisation and Referrals. See section 5.

13.2 Training your staff

Alert, well-trained staff members are your frontline defence against card fraud and can significantly reduce the risk of financial loss to your business.

If you or your staff allows fraud to take place through carelessness, you could lose money and we may even stop processing card payments for you.

Please make sure your staff read this guide carefully, and any other fraud prevention publications we send you.

Withholding payments

If we are suspicious about a transaction you have processed or we believe that a transaction may be fraudulent, we may hold back payment while we investigate. The money will not be returned until we have confirmed that a genuine transaction has been processed and it was for the goods or services provided by you (and not any third party) and which you advised you would be providing on your application form. There is no set time limit for the investigations to be resolved, but we will keep you informed throughout.

© Worldpay 2015. All rights reserved

13.3 Card present transactions

These are face-to-face transactions where your customer and their card are with you at the point of sale. Find out more in Card Present Transactions, section 4.

13.3.1 Look out for fraud warning signs

Be aware of how customers normally behave when they are shopping. If you notice anything out of the ordinary, or something that just doesn't feel right, it could be a sign of potential fraud, so act on your instincts and don't go ahead if you are suspicious. Look out for...

- **Random, careless or bulk purchases** – Most customers ask questions and, for example, try on clothing, but a fraudster will just buy goods that can be easily re-sold.
- **Rapid repeat visits** – A customer who returns to buy more in a short period of time may be making the most of the fact that the card has been accepted already.
- **Nervous or hurried customers** – They may be worried about being caught.
- **Cards signed in felt-tip pen** – This can be used to disguise the original signature – remember all cards should be signed in ballpoint pen.
- **Interruptions** – A customer who tries to distract you during the transaction, and who seems fully conversant with how the authorisation process works, may be trying to prevent you from noticing something suspicious. Never turn your attention away from the terminal once you have started processing the transaction, as you may miss prompts on the screen, or miss a fraudster attempting to interfere with the terminal.
- **Fake authorisation calls -** Neither Worldpay nor the card issuing bank will EVER call you during the processing of a transaction to provide you with an authorisation code. If this happens this will be an attempt by fraudsters to force through a transaction, and will result in a loss to your business if the transaction is charged back. If you receive one of these calls please cancel the transaction (if safe to do so) and perform a 'Code 10' call.
- **Worldpay, Police or other 'official' impersonation –** You should never receive a phone call from the Worldpay authorisation centre, the police, your terminal provider or any other official, requesting you to provide any card details over the phone. None of these organisations will ever ask for details over the phone, so these will be an attempt by fraudsters to gain card details from you. If you receive one of these calls, please report it to the Worldpay Helpdesk.

13.3.2 Take extra care when a signature is needed

- Nearly all cards in the UK now use chip and PIN technology, but you may sometimes come across cards that need to be verified using a signature rather than a PIN. Knowing when these cards can be used and their security features will help you to identify genuine transactions and also to spot potential fraud. Take extra care when accepting these transactions because you could be financially liable if a transaction is confirmed as invalid or fraudulent.
  In certain circumstances, you can accept:
- **Chip and signature cards** – You should only use a signature to verify a transaction in exceptional cases. The main ones are if the customer has a non-UK-issued card, or an impairment that means they need to sign. Follow the prompts on your terminal. **Magnetic stripe and signature cards** – These will mostly be non-UK-issued cards from countries that have not yet upgraded to chip and PIN. Follow the prompts on your terminal.

13.3.3 Some basic fraud checks to use when a signature is required

If you do carry out a transaction using a signature as verification, you should take extra security precautions:

© Worldpay 2015. All rights reserved

- Check the security features of the card. Find out more in our Card Recognition Guide. See section 16.
- Check the cardholder's signature matches that on the back of the card.
- If possible, check that the spelling on the card is the same as the signature – fraudsters sometimes don't spell the name correctly.
- Check the title on the card matches the gender of the person presenting it.
- Check the signature strip for tampering – has another strip been placed over the top of the original one? If the word "void" appears on the strip, this could be an indication that the genuine signature has been removed and a substitute used.
- If you have an ultraviolet (UV) lamp, put the card under it and check the appropriate inbuilt security feature
- While the point-of-sale receipt is printing, check the last four digits of the card number on the receipt match those on the front of the card. If they don't, make a 'Code 10' call.

13.3.4 If the Authorisation Centre asks you to retain the card

Explain politely that the card issuer has asked you to hold onto the card. Your own company policy will decide whether you detain the cardholder or call the police. Never put yourself, your staff or the public at risk.

Even if the Authorisation Centre does not ask you to retain the card, you may decide that a card or a transaction is suspicious – for example, if you have identified it as counterfeit. Card thieves act fast, and will often try to use a card before the owner notices that it has gone.

There may be a reward for recovering a card that is being misused.

13.3.5 Preserving evidence

The physical card which is presented to you and used fraudulently may need to be used as evidence. Treat them with care and you will make it easier for the police to catch and prosecute the thieves.

Please check that these instructions are in line with business policy. If you are responsible for company policy, you should consider incorporating this advice as far as possible into staff training. If staff come into contact with criminals, it is far better – and less stressful – if they are prepared for the possibility and have an agreed process to follow.

- **Preserve the card:**
- **Don't cut the card in half**
- Handle it by the edges so as to preserve fingerprints.
- Cut off the bottom left-hand corner (as seen from the front) – Don't cut it in half
- Don't damage any other part of the card.
- Handle it as little as possible and place it in a plastic bag or envelope until you can give it to the Police.
- **Keep the voucher or receipt:**
- Keep the best copy possible.
- Don't pin or staple anything to it.
- Put it in the same envelope/bag as the card to give to the Police.
- **Keep the video/CCTV:**
- If you have a video surveillance system, keep the tape and give it to the Police.
- Keep a copy if you can.
- **Note down a description of the person who presented the card**
- Write down the details immediately while they are fresh in your memory.
- Think about the person's unique features such as their accent, scars, tattoos and body language rather than the clothes they are wearing.

© Worldpay 2015. All rights reserved

13.3.6 Involving Police

If your company policy dictates, inform the police **via *www.actionfraud.police.uk***

If the Police ask for the card you should:

- Allow the Police Officer to take it.
- Take a note of the officer's name, number and station.
- Obtain the Crime Reference Number.
- Get a receipt and keep it safely as this may enable you to claim a reward.

13.3.7 If someone leaves a card behind

- Keep it somewhere safe for at least 24 hours, in case the cardholder comes back for it.
- If someone comes to claim the card, ask them for signed proof of identity, such as a driving licence or other cards, and compare the signatures.
- Ask them to sign a blank receipt and compare the signatures. Then destroy the receipt.
- If you are then happy with the cardholder's identity, give them the card.
- If you are suspicious, ask them to come back with additional proof of identity. If you are still not satisfied when they come back, call the Authorisation Centre (number detailed in Section 1.5.1) and say "This is a 'Code 10' call". The operator will talk you through the process.
- If the cardholder does not return to reclaim the card, please send it to us to be cancelled. First cut the card into two pieces. Looking at it from the front, cut off the bottom left-hand corner. **Do not** cut through the signature strip, magnetic stripe, hologram or chip. Then send the pieces with a short note giving your address and the date you found the card to:

  Card Rewards Section
  Gateshead Card Centre
  5th Avenue
  Gateshead
  NE11 0EL
  United Kingdom

13.3.8 Rewards

Depending on the circumstances, there may be a reward for cards you hold on to when asked by the Authorisation Centre.

Return these cards to

Card Rewards Section
Gateshead Card Centre
Victory House
5th Avenue
Gateshead
NE11 0EL
United Kingdom

When you send the card, please also provide the following information:

- The name and address of your business
- Your Customer Number and telephone contact details
- The date on which you kept the card
- The name on the card
- The card number (the long number across the centre of the card)
- Details of the person who should get any reward

© Worldpay 2015. All rights reserved

If the police take the card as evidence, include the Police Officer's details in the above list plus the date reported and the Crime Reference Number. Keep a copy of these details.

13.4 Card Not Present Transactions (CNP)

If you are suspicious of the card, cardholder or circumstances of the sale at any time we recommend you do not continue with the transaction or send out the goods. If you decide not to proceed once you have already processed the transaction, you will need to make a refund to the card. See Refunds, section 6.

CNP transactions are considered high-risk because you have no opportunity to physically check the card or meet the cardholder. Although most CNP sales are genuine, this type of transaction is appealing to fraudsters who want to obtain goods to resell easily for cash. So take extra care and consider the risks before you process CNP payments, because you will be financially liable if a transaction is confirmed as invalid or fraudulent.

13.4.1 Look out for fraud warning signs (MOTO)

Here are some signs that a transaction is likely to be fraudulent. Get to know them and make sure that all members of your staff recognise them too. Sometimes the first sign of fraud can just be a general feeling that something isn't quite right. If that happens, act on your instincts and don't send out the goods until you've carried out further checks.

- **Multiple or bulk orders** – Watch out for customers buying lots of the same item – either in the same transaction or separately.
- **First-time customers who place multiple orders** – The risk of fraud is smaller when dealing with customers you know.
- **High-value orders** – Orders larger than normal may indicate fraud. High-value items such as jewellery or electrical goods are often targeted by fraudsters because they are easy to resell, so take extra care with this type of transaction.
- **Hesitant customers** – Customers who seem uncertain about personal information, such as their postcode or spelling of their street name, could well be using a false identity. Also watch out for customers being prompted when giving the requested information.
- **Same name, different title** – Could your customer be using the card of a family member?
- **Sales that are too easy** – Be suspicious if a customer is not interested in the price and/or detailed description of the goods, but is only interested in delivery times.
- **Suspicious card combinations such as:**
    - Transactions on several cards where the billing address matches but different/various shipping addresses
    - Multiple transactions on a single card over a very short period of time
    - Multiple cards beginning with the same first six digits offered immediately after the previous cards are declined
    - Customer offering multiple different cards one after another without hesitation when previous cards are declined
    - Orders shipped to a single address but purchased with various cards
    - Requests for urgent delivery – This could be genuine, but rush orders are common in fraud scams that aim to obtain goods for quick resale before the card is reported stolen.
    - Overseas shipping address – Be careful when shipping overseas, especially if you are dealing with a new customer or a very large order.
    - Different shipping address – Orders where the shipping address is different from the billing address may be legitimate (for example, when sending flowers or a birthday present) but requests to send goods to hotels, guest houses or PO boxes are often associated with fraud.
    - Duplicate shipping address – Has the shipping address been used previously for similar orders? Be cautious if you identify the same delivery address being used.
    - Requests to send funds abroad – This is typically a request for money transfer or other payment method to pay for couriers, interpreters or other similar services or requests.

© Worldpay 2015. All rights reserved

For example, a request to take a payment greater than the value of the goods/services being purchased, where the customer requests the surplus funds to be sent overseas or to another bank.

Authorisation does not guarantee payment. It simply means that at the time of the transaction the card has not been reported lost or stolen and that there are sufficient funds available. Card thieves act fast and will often try to use a card before the owner notices it has gone. Find out more about Authorisation And Referrals. See section 5.

13.4.2 Look out for fraud warning signs (eCommerce)

Here are some signs that an eCommerce transaction is likely to be fraudulent. Get to know them and make sure that all members of your staff recognise them too. And remember that the first sign that something is wrong can just be a general feeling of unease. If that happens, act on your instincts and carry out further checks.

- **A risk alert** from the payment service provider or acquiring bank. This indicates that there is a cause for concern and that further checks are required before an order is fulfilled.
- **Multiple transaction attempts** using the same or similar shopper details, such as name, e-mail address or IP address across one payment.
- **Different shopper details with one element the same** – such as ten transactions from the same IP address giving different shopper names and e-mail addresses.
- **Multiple cards used by same shopper**, especially where the card numbers are similar.
- **Obvious 'card testing'**, where the last four or eight digits of cards in a series of attempted payments contain similar numbers, or the card numbers are cycled repeatedly in a rough pattern or sequence.
- **Nonsensical shopper details**, such as 'dgsgsgdf@dsgsd.com' as a shopper e-mail address or 'gdfgdfgfg' as a shopper name or billing address
- **High-value transactions**, especially where the amount is out of the ordinary for your usual daily processing amounts.
- **Mismatching Card Security Code** (CSC) or **mismatching Address Verification Check** (AVS). Consider rejecting orders that carry mismatches or carry out further checks.
- **Mismatching combination of billing country, issuer country and IP country**, especially, but not limited to, instances where the payment details are from any country or area which is associated with high risks of online fraud.
- **A delivery country that's out of the ordinary** for your business and regarded as high-risk
- **Use of 'freemail' e-mail addresses**, such as Yahoo!, Hotmail, MSN, Gmail, Live or YMail. Although these e-mail services are completely legitimate, they are often associated with fraud attempts because they are easily available and relatively anonymous.
- **An e-mail address** that bears no relation to the shopper name.
- **A request to hurry** the order shortly after it has been placed.
- **A request to send anything** of the same value.
- **Indiscriminate buying** or unusually large orders that seem out of the ordinary.
- **A request to change the delivery address**, especially to a high-risk area/country (see above).
- **Shoppers who give card numbers by e-mail** and seem reckless with sensitive information. Sending full card numbers by unencrypted e-mail is not PCI-DSS-compliant.
- **Shoppers who give a high number of card details** or lots of different billing information.
- **A request to conceal or alter payment details**, or the way in which the payment is made, to make it look more legitimate.
- **General inconsistency** between the shopper's name, e-mail address, or the way they communicate and the kind of goods or services being purchased.

© Worldpay 2015. All rights reserved

13.4.3 How to combat eCommerce fraud

One of the best ways to combat fraud is to be alert and to check up on anything that seems suspicious. Here are a few other important ways to help reduce the exposure of your business to fraud.

- **Make the most of industry tools** like Cardholder Authentication, 3D secure (MasterCard SecureCode, Verified by Visa and American Express SafeKey, CSC and AVS checks, Risk Guardian and the Risk Management Module. Ask the Worldpay Helpdesk or your Payment Service Provider (PSP) for more information.
- **Screen transactions** and consider applying risk scoring and alerts to flag suspect activity that merits further checks. You may be able to design your own in-house system – or ask your PSP.
- **Compare new shopper information** to data you already hold. Keep records of previous fraud attempts and chargebacks and reject orders where there are matches.
- **Look for patterns** such as similarities between transactions and repeat use of the same shopper name, e-mail address or IP address – and investigate anything suspicious.
- **Verify the shopper's identity** if you are suspicious. Test their contact details to see if they work – send an e-mail and call the telephone number. You may also ask for copies of utility bills, card statements, passport or driving licence (with any sensitive details obscured).
- **Establish a fraud policy** setting out what should be done if fraud is suspected and ensure that all members of your staff are trained to act.

13.4.4 What else to consider

- **Establish authenticity of customer**
  It is advisable to establish the authenticity of a customer before delivery by obtaining residential address, telephone number, etc. – perhaps checking with data that is available publicly.
- **Search the Internet for imposters**
  We recommend that you regularly search the Internet for websites using similar names to your own. These may have been set up to impersonate your company illegally.
- **Use expert input**
  A number of companies, such as PSPs, provide services to help you to look out for potential fraudulent transactions. Fraud-screening measures include:
  - Parameter-based technology to filter card transactions
  - Third-party name- and address-checking techniques
  - Methods of validating cardholder data

To find out more about how we can help, contact us or get in touch with your PSP.

13.4.5 Additional security

We recommend you take full advantage of the additional security checks available through your terminal - Card Security Code (CSC) and Address Verification Service (AVS).

If we have supplied your terminal, it should prompt you for the information needed to make the additional checks – if you have any other terminal, you may need to speak to your supplier to find out how to take advantage of these.

These additional checks via your terminal cannot confirm cardholder names and therefore you should take additional steps to do so if you are in any way unsure about the transaction.

One option would be to request a landline number and checking via a directory enquiries service.

13.4.6 Delivery

There are also opportunities for fraud at the delivery stage. You should have your own policies when it comes to reducing this type of fraud, but here are a few recommendations that can help.

© Worldpay 2015. All rights reserved

- Make sure that goods are always delivered to the billing address (preferably inside your customer's premises) and to the person set out in the order.
- Obtain a signature from the cardholder as proof of delivery – this can be used as evidence in the event that a dispute subsequently arises.
- Don't release goods to third parties such as friends or relatives of the cardholder, taxi drivers, couriers not arranged by your business, messengers, etc.
- If using your own staff for delivery, consider using a mobile terminal (see our website for details of our mobile card machines) to enable you to take the transaction as card present when the goods are delivered.
- If a cardholder changes their mind and wishes to collect the goods, they should attend your premises in person and produce their card. You must either cancel or refund any previously-completed CNP transaction and process a new card present transaction.

© Worldpay 2015. All rights reserved

14 Reconciling Your Invoice

If you have a Worldpay terminal, you need to complete an end of day report at the end of each day's trading and within your allocated banking window.

Completing an "end of day" report checks that the transactions have been processed correctly and are not stored in the terminal, which could delay the funds being credited to your account. You will also find it very useful to help reconcile your accounts.

If you're unsure of how to do this, instructions can be found in our terminal user guides:

Your Worldpay invoice details all the transactions processed that month, plus any associated charges. Your invoice for the period will be available in the first week of each month and we will debit your account on or around the 18th of each month.

See Understanding Your Bill on Worldpay.com for further details.

14.1.1 Electronic Management Information (MI)

In addition to your monthly invoice, if you've signed up to receive detailed Monthly Electronic Management Information (MI) you will receive this information via email during the first week of each month.

To receive MI you must have:

- Registered your e-mail address with us
- Access to the internet
- Microsoft Excel 97 (or later version)

To register, write to the following address requesting that your account is set up with access to Electronic Management information. You will need to quote your customer number and provide the email address which we should use to send the monthly MI email.

Amendments
Worldpay
Victory House
Fifth Avenue
Gateshead
NE11 0EL

Opening MI files

To open the MI files you will need download a formatter to convert the file to a user friendly version.

How to download and install the File Formatter

- Download the file formatter or paste www.worldpay.com/sites/default/files/reconciling-your-invoice.xls into your web browser
- If a message about macros appears, select "Yes – enable macros"
- Be patient – this may take a minute to load
- Save the spreadsheet to your pc/file server
- Click the "Add IMIX toolbar" button on screen

You'll only need to do this once – File Formatter will remain on your computer

© Worldpay 2015. All rights reserved

When you get your monthly MI:

- Open the file in Excel
- Click on the IMIX CVS File Formatter toolbar
- The file will then be converted to a user-friendly format

14.1.2 Premium Transaction Charges

When applicable your monthly invoice will summarise the premium charges that are payable. If required the MI (see previous section) will provide more detail. See Understanding Your Bill for further details.

14.1.3 More Information

Further information, Frequently Asked Questions and a video overview are also available on our web site. See Understanding Your Bill.

© Worldpay 2015. All rights reserved

15 Chargebacks

Card transactions are sometimes disputed by the cardholder or the card issuing bank, for example goods not received, transaction not recognised or authorised. When this happens we may contact you requesting further information by sending a Request For Information (RFI) letter.

If you are not able to supply the information requested by us or in the timescales we specify then it is likely that an RFI may turn into a chargeback which you may be held liable for, even if you have proof that the transaction was genuine.

Depending on the nature of a dispute you may sometimes get a chargeback letter without an RFI. This can happen when it's clear that the right process has not been followed, for example, if you have taken a payment above your floor limit without obtaining a valid authorisation or an eCommerce transaction without cardholder authentication (e.g. Verified By Visa or MasterCard SecureCode), and the cardholder has declared they did not authorise or participate in the transaction.

Where there is a valid chargeback we will write to you to let you know and Worldpay will debit your nominated bank account with the value of the disputed transaction, quoting the same unique reference number as in the chargeback letter. You are responsible for making sure sufficient funds are in your nominated bank account to meet the chargeback. Failure to do so could result in your card processing facility being withdrawn.

15.1 Why chargebacks happen

Here are some of the most common reasons for chargebacks, but this is not a full list. If you are not sure about the reason for a chargeback, please contact the Worldpay Helpdesk and select the chargebacks option.

15.1.1 Disputed payments

Some common reasons for disputes include:

- The cardholder claims someone was using the card without his or her knowledge or states that he/she does not recognise the transaction. It could have been stolen and used fraudulently – particularly for MOTO and eCommerce transactions
- There is a processing error, such as the wrong card number or wrong amount was keyed
- The cardholder disputes some other aspect of the transaction, for example non-delivery, late delivery, unsatisfactory goods or services, or the wrong size/colour/price. For further information about Goods And Services Disputes in Section 15.1.8

15.1.2 Wrong or suspect card details

There is also a high risk of a chargeback if there was a mistake when the transaction took place. Other common problems are:

- The card is not valid – for example it is out of date
- No signature
- Details on the terminal receipt or voucher don't match the card – i.e. the embossed details on the card do not match the details on the electronic receipt or the details have been entered incorrectly by hand -Primary Account Number (PAN) key entry.
- Wrong process
  - Your customer has been billed twice for the same sale.
  - The transaction was by PAN key entry, but a separate imprint and signature was not taken on a back-up paper voucher. See using paper vouchers, section 8.1
  - The sale required authorisation but it was not obtained.
  - An authorisation call was made, but the sale was not authorised.

© Worldpay 2015. All rights reserved

- You have submitted another authorisation request for the same transaction that had already been declined by the Issuer.
- Two or more transactions have been made on one card, for one sale in order to avoid authorisation or referral of the whole as one transaction - known as a 'split sale'.
- You have made a sale not covered by your contract with us – remember you will need an agreement with us which allows you to offer MOTO or eCommerce sales.
- An electronic transaction has been stored on your terminal but not sent through to Worldpay within three working days (unless this has been agreed in advance).
- You have keyed card numbers manually or used paper vouchers when your terminal was working.
- You have processed a card that is not covered by your contract with us.
- You have taken a non-UK-issued Maestro card and keyed in the number by hand.
- You have taken an Electron or non-UK-issued Maestro card and used a paper voucher.

- A problem with your response to an RFI
  - You have not replied to an RFI letter within the given timescales.
  - You have replied to an RFI letter with illegible or incomplete documentation.
- A problem with a paper voucher
  - The signature on the voucher is missing, card details not imprinted, impossible to read, or doesn't match the card.
  - The voucher supplied doesn't match the customer's voucher.
  - The voucher is missing details, such as the date, amount or signature.
- A problem with mail order
  - You have not kept any paperwork signed by your customer that proves the goods were delivered correctly.
- A problem with service or changes to specification
  - You have not obtained confirmation from the cardholder that a service has been completed to their satisfaction.
  - There have been changes in the price or specification and you have not obtained the cardholder's signature in agreement.
- Other problems
  - In some other way, you have gone outside your Contract with us

15.1.3 Goods and services disputes

These types of chargeback disputes can be difficult to defend and therefore if a customer contacts you with a dispute you should retain accurate records of what is discussed or agreed. Where possible, ask the customer to put the complaint or query in writing/e-mail and have the customer agree in writing to any resolution agreed. Proving the content of a telephone conversation at a later date is virtually impossible and the Card Schemes do not accept recordings of telephone conversations as evidence.

It is important to be aware that the cardholder does not always have to physically return the goods to you for a chargeback to be correctly raised.

Please also be aware that the use of 3D Secure protects you from fraud-related chargebacks, however chargebacks could still result from goods and service disputes.

15.2 What if cardholders get in touch with you directly?

You and your customer may come to an agreement to issue a refund but this will usually be prior to a chargeback being raised. If you wish to make a refund after receiving a chargeback or an RFI letter you should contact the Worldpay Helpdesk to discuss this as a response to the card issuer will still be required.

© Worldpay 2015. All rights reserved

- If the customer just wants their money back under your returns policy, find out more in Refunds. See Section 6
- Never give a refund for any other reason to the cardholder without checking with the Worldpay Helpdesk.
- If you have received an RFI or chargeback letter, you must never make a refund to the cardholder without **checking with the Worldpay Helpdesk first.**

15.3 What is a Request For Information (RFI)?

It's when a card issuer or cardholder instructs us to ask you for details about a specific transaction. If this happens, we will send you an RFI letter asking you for the relevant transaction records.

A card issuer does not need a specific reason to ask for information about a transaction.

We will give you as much information as possible to help you trace the payment. This will include the transaction date, card number and transaction reference. The cardholder's name and address will not be given, in line with the UK Data Protection Act.

15.3.1 What to do if you receive an RFI letter

If you receive an RFI letter, you must send us the information we ask for as soon as possible. You will have a set time to reply – **it is very important to respond by the date given or timescales specified.**

- Response times are set by us to ensure there is sufficient time to provide a response to the card issuer within the timescales set by the Card Schemes. As a result, we cannot give you extra time to respond
- If you don't respond or are late with your reply, a chargeback debit may be applied to your account.
- If you have Worldpay Online, you will receive an e-mail prior to receiving an RFI letter.

15.3.2 Information to supply if you receive an RFI letter

The more information you give us in response to an RFI letter, the more likely it is that we will be able to answer the card issuer's query or defend your position. However, producing all the documentation you are asked for does not always prevent the card issuer making a chargeback.

You should supply:

- A copy of the invoice for the goods or services provided
- Any documents signed by the cardholder
- Any terms and conditions issued at the time of the sale. These should be signed by the cardholder
- If the goods were delivered – evidence of delivery. This should be signed by the cardholder
- For a rental – the rental agreement
- For a refund – the refund voucher
- For MOTO sales – a copy of the sales receipt or Mail Order Telephone Order schedule
- For eCommerce sales – a copy of the source documentation showing all the data captured at the point of sale, including the card number. You may need to print screen images. If necessary, ask your Payment Service Provider (PSP) to help
- For delayed and amended charges (i.e. minibar charges at hotels, parking tickets / damages for vehicle rentals) – a copy of the cardholder agreement to be billed for the additional charge
- Any additional comments relevant to the transaction or dispute – particularly where the cardholder may have approached you directly. You should include details of the outcome of this approach.
- **The transaction documentation should include:**
- Truncated card number (first 6 and last 4 digits of the customer's card number)

© Worldpay 2015. All rights reserved

- Unless it is a PIN verified transaction, the cardholder's signature (in both face-to-face transactions and transactions by post or fax).
- Transaction amount
- Transaction date
- Your trading name and location
- Card expiry date
- Cardholder name and address (generally for Mail Order Telephone Order and eCommerce transactions)
- Description of goods/services provided

15.4 Secure record keeping

See Keeping Records, section 2.7, for details of how receipts, paper vouchers and other high security items must be securely stored.

15.5 If the post is disrupted

If there is a problem with the post, your letters may be delayed, but will be sent to you as soon as possible. Even if this written explanation is late reaching you, the chargebacks will be debited from your account as usual.

15.6 Disputing a chargeback

You can dispute a chargeback that has been applied to your bank account. You will need to provide information to prove that the transaction was authentic. Worldpay will consider any information you can provide within the required timeframes proving that the transaction is authentic. However your account will only be credited if the evidence provided meets the rules set by the Card Schemes.

Even if all procedures have been correctly followed and documented, this does not guarantee that you will succeed in disputing a chargeback. The technology we use is designed to ensure that chargeback enquires are resolved efficiently with minimum disruption to your business.

© Worldpay 2015. All rights reserved

16 Our Other Services

In addition to sales transactions, Worldpay also allows you to accept card payments for the following services:

- Hotel Services
- Vehicle Rental Services
- Bureau de Change
- myCurrency
- Tax free shopping

16.1 Hotel Services

We offer two card payment services that can help you to run your hotel business efficiently by enabling your guests to make guaranteed reservations over the phone or online and to save time with express checkouts.

Guaranteed reservation

With our guaranteed reservation service, hotel guests who give their card number when they make a booking are guaranteed a room. It also entitles you to charge the card for one night's stay if the guest does not arrive, or cancels their booking after an agreed deadline or with insufficient notice

To use this service, you need agreement(s) with us to process MOTO transactions and eCommerce, if accepting bookings over the Internet.

16.1.1 Which cards can I accept for guaranteed reservations?

You can accept:

- MasterCard
- Debit MasterCard
- Visa
- Visa Debit
- JCB
- Diners/Discover

You cannot accept:

- Maestro
- Visa Electron

16.1.2 What details do I need from the cardholder?

When a guest calls to make a guaranteed reservation, you will need to take their:

- Card type
- Card number – the long number across the centre of the card
- Name as it appears on the card – including any initials
- Card expiry date
- Full postal/billing address, including postcode, as it appears on their statement
- Contact address – if different from above
- Contact telephone number
- Planned date of arrival and length of stay
- Number and type of room(s) wanted

Never ask for a customer's PIN.

© Worldpay 2015. All rights reserved

16.1.3 The Data Protection Act 1998

Please remember that, if you are collecting personal data like the above, you need to register as a data controller. Your failure to do this and any subsequent action that may be taken against you will not be the responsibility of Worldpay.

16.1.4 What information must I give the cardholder/guest?

When the booking is made, you must provide the cardholder with the following information in writing:

- Rates for the room(s) they have booked
- Booking conditions
- Hotel address
- Your internal reservation code for their guaranteed reservation

You must also explain the following conditions:

- The deadline for cancellation is 6pm local time on the booked date of arrival.
- If the guest cancels later than this, they will be charged for the night.
- You can set your own deadline earlier than this, up to a maximum of 72 hours before 6pm on the arrival date. If this is your policy, you must explain this at the time of booking and confirm it in writing at least three days before the arrival date.
- If the guest fails to arrive at the agreed time, the reserved room will be held until noon on the day following the reservation date.
- If they do not arrive during this time, they will be charged for one night's stay, and the rest of the booking will be cancelled with no charge. This is called a 'no-show'.

For eCommerce transactions you must also provide copies of the relevant web pages detailing the terms and conditions of the booking, plus the actual website address.

16.1.5 What if a guaranteed reservation is cancelled?

If a guest cancels their booking within the deadline or with sufficient notice, you must not process a card payment. You should also provide them with this information in writing:

- A cancellation reference number, which you should also keep on file
- If the cardholder asks you to, you must include the cardholder's name, the last four digits of the card number, the card expiry date and your own cancellation code in this written confirmation.

16.1.6 'No-shows' and late cancellations

If a guest fails to appear before noon on the day following their reservation, or calls to cancel the booking after the deadline, you are entitled to charge their card for one night's stay in the room or rooms that they reserved. To do this:

- Follow the instructions in Card Not Present Transactions, using the information the cardholder gave when accepting the booking.
- On the transaction receipt, write "NO SHOW".
- Under 'total' enter the room rate for the room(s) that they booked.
- Send a copy of the bill for the 'no-show' booking to the billing address the cardholder gave when booking.

16.1.7 What if the accommodation has been overbooked?

If a guest has made a guaranteed reservation but the room is not available when they arrive, you must provide them with:

- Comparable alternative accommodation
- Transport to the alternative accommodation and between establishments, if requested

© Worldpay 2015. All rights reserved

- Forwarding of all messages and calls to alternative accommodation
- Two three-minute telephone calls, free of charge

If you do not provide these services, you may be excluded from taking MasterCard, Visa or JCB payments for guaranteed reservations in the future.

16.1.8 Keeping records

You must file copies of the following and keep them securely for a minimum of 13 months in case there is a query later or the details are required to help to defend a chargeback.

- Cardholder's name, address and card number
- The terms and conditions for the reservation, as provided to the cardholder at the time of the booking
- The confirmation code
- Transaction receipt, if a night's stay is charged
- Hotel bill
- Any correspondence relating to confirmations received from the cardholder acknowledging the terms and conditions of the booking

16.1.9 Express checkout

This convenient service means that when guests are ready to leave, they can return their keys and go without waiting for their bill to be made up. It is very important to follow the correct procedure carefully to reduce the risk of chargebacks.

Which cards can I accept for express checkout?

You can accept:

- MasterCard
- Debit MasterCard
- Visa
- Visa Debit
- JCB cards
- Diners/Discover
- American Express (if you have a supplementary agreement)

You cannot accept:

- Maestro
- Visa Electron cards

How do I use express checkout?

When the guest arrives:

- Ask them whether they would like to use the service – not all guests will and some prefer to check their bill before paying it.
- If they agree, ask for the card with which they intend to settle their bill.
- Ask your guest to write down the billing address for the card. This is normally their home address, but some company cards are billed to the company address.

Processing the transaction

When you have verified the card and the cardholder, follow the instructions in Card Present Transactions – Chip and PIN.

- The expected amount of the bill (the room rate, multiplied by the number of days accommodation) needs to be pre-authorised. Find out how to process pre-authorised transactions in your Terminal User Guide.
- Explain to your guest that the bill will be debited to their card account after they have left and that there is no need to pay on checking out.

© Worldpay 2015. All rights reserved

- If the transaction is not authorised, you will need to ask your guest for another method of payment. If they give you another card, you will need to verify this again before starting a new transaction.

Maestro cards do not support pre-authorisation requests.

After your guest has left

- Work out the final bill.
- Follow the instructions to complete the transaction using your terminal.
- Send the bill and a copy of the terminal receipt to your guest at the billing address supplied. You must do this within three working days of the transaction.
- If the final bill is higher than the pre-authorised amount, you will need to complete a top-up authorisation. Find out more in Authorisation and Referrals in Section 5 or in your Terminal User Guide
- If the top-up authorisation is declined, you will need to contact your customer and ask them for another method of payment.

Delayed or amended charges

There may be times when you need to process extra charges or change the amount agreed because of other costs incurred during the stay. These extra costs are called delayed or amended charges.

For hotel stays the following services may be the subject of a delayed or amended charge transaction:

- Room charges
- Food or beverage charges

A delayed or amended charge transaction must be completed within 90 calendar days of the transaction date of the previous transaction to which the delayed or amended charge transaction relates.

Processing the transaction

When carrying out a delayed or amended charge transaction, you must:

- Include the words “Signature on File” on the Transaction Receipt.
- Send a copy of the transaction receipt to the cardholder at the cardholder's address.

Disputes (including chargebacks)

In the event that we receive a disputed card transaction, we will write out to you requesting documentation to assist us in defending the dispute. Should the documentation not be supplied to us within the timescale indicated in the letter this will result in a chargeback debit to your bank account.

You must provide evidence that the charges billed were incurred by the cardholder during their stay.

If you do not have any documentation to do this, we will not be able to defend a dispute on your behalf and a chargeback debit will be processed to your bank account.

Please note that any transaction processed in a card not present environment is taken at your own risk and can be subject to a chargeback dispute for which you may be liable and would result in a debit to your bank account.

16.2 Vehicle Rental Services

Being able to accept card payments for vehicle rentals gives you and your customers flexibility. It also offers you the added security of pre-authorising payments before the customer takes the vehicle away.

© Worldpay 2015. All rights reserved

16.2.1 Before you start

You must let us know if you intend to accept card payments for vehicle rentals, because there are special requirements for these transactions.
To minimise disputes and chargebacks, you should read this section thoroughly and ensure that you understand the specific requirements and risks of these transactions.

16.2.2 What information must I give the cardholder?

When a customer rents a vehicle from you, you must provide them with a **rental agreement** that includes all applicable terms and conditions for the rental, including:

- Cancellation policy and procedures
- Reserved vehicle rental rate
- Currency of the transaction
- Name and location of where the vehicle is to be collected from
- 'No-show' policy and procedures
- Any extra charges that they may be liable for, such as damages, parking tickets, no show policy and procedures and any limited refund policies

16.2.3 Make sure that the cardholder signs the rental agreement to confirm that they have read and understood the terms and conditions before you process any transactions.

When a customer comes to collect the rental vehicle, you need to do two main things before they take the vehicle away with them – get their agreement to the rental agreement and pre-authorise the transaction.

- **Get their agreement to the rental agreement**
  - Ask your customer to read the terms and conditions and sign the rental agreement.
  - Make sure that their signature is on the same page as the terms and conditions and details the card number to be used for payment for the rental and to be used in the event of any delayed and amended charges.
  - Manually imprint the card on the rental agreement as evidence of the agreed charges.
  - You will need the cardholder's separate agreement to process any additional charges.
- **Pre-authorise the transaction** before the rental period begins you need to make an estimated authorisation request. This is called pre-authorising the transaction and should be based on the:
  - Vehicle rental period
  - Vehicle rental rate and associated taxes
  - Anticipated mileage
- **Process the transaction**
  - If the pre-authorisation request is approved, you will be given an authorisation code. You can use this authorisation code when you process the payment at the end of the rental period. Find out how to process pre-authorised transactions in your Terminal User Guide.
  - If the pre-authorisation request is declined, you will need to ask your customer for another method of payment.
- **To reduce the likelihood of disputes you should let your customer know:**
  - The pre-authorisation amount
  - That the available funds on their card will be reduced by this amount
  - That the final bill may be different to the pre-authorisation amount

If the rental period is extended during the rental, additional amounts must be authorised via top-up authorisations. This will ensure that funds are held available when you come to charge the card. You will also need additional authorisation to process the payment if the final bill is more than 15% higher than the pre-authorised amount. Find

© Worldpay 2015. All rights reserved

out about top-up authorisations in your Terminal User Guide.

Maestro cards do not support pre-authorisation requests.

Authorisation does not guarantee payment. *It simply means that the card has not been reported lost or stolen and that there are sufficient funds available at the time of the transaction. Find out more about Authorisation. See section 5*

16.2.4 How to process payments

- You should process the payment after the customer has returned the vehicle.
- The exception is for rentals of longer than 14 days. To minimise risk and ensure that payments are processed successfully, we recommend that after a 14-day rental period you close the account and process the required payment up to that date.
- If the final bill is higher than the pre-authorised amount, you will need to complete a top-up authorisation. Find out more in Authorisation and Referrals in Section 5 or in your Terminal User Guide.
- Do not include charges for damages or insurance deductibles in the payment. These charges need to be processed separately as delayed or amended charges.

16.2.5 What if the customer cancels or doesn't show up?

- **If a customer cancels their reservation**
  - You must not process a charge to the card for the booking. If you do, there is likely to be a dispute that may result in a chargeback. If your rental agreement says that a cancellation charge will apply, you will need to contact the customer to arrange for payment by another method.
- **If they do not cancel, but fail to collect a booked vehicle**
  - If your customer fails to collect their vehicle within 24 hours of the collection time and did not properly cancel the reservation in accordance with the agreed cancellation policy, you are entitled to charge their card up to the value of one days rental:
    - Follow the instructions in Card Not Present Transactions, using the information the cardholder gave when making the booking.
    - On the transaction receipt, write "NO SHOW".
    - Under 'total' enter the rental rate for the vehicle(s) that the customer booked.
    - Send a copy of the bill for the no show booking to the billing address the cardholder gave when booking.

16.2.6 Delayed or amended charges

There may be times when you need to process extra charges or change the amount agreed because of damages or other costs incurred during the rental period. These extra costs are called delayed or amended charges.
The way to process delayed or amended charges is different for Visa and MasterCard. It is very important to follow the correct procedure as detailed below.

Visa transactions

A vehicle rental company may process delayed or amended charges for fuel, rental damage, theft, 'no-shows', parking tickets and other traffic violations. The cardholder can only be charged for transactions incurred during their rental period that they agreed to in the pre-rental agreement. These should be processed by you as soon as possible following the original transaction, and in any event no later than 90 days from then for Visa transactions.

© Worldpay 2015. All rights reserved

Before you can process these charges you must first provide evidence to your customer to support any claim, supplying documentation from the relevant civil authority including:

- The licence number of the rental vehicle
- Time/date of the violation
- Amount of the charge, in the local currency of that civil authority
- The statute that was violated
- Evidence to prove the cardholder had read the terms and conditions and accepted responsibility to pay for any delayed or amended charges incurred during their rental
- Evidence to prove the cost of any charges, as well as supplying proof that the vehicle was returned damaged or short of fuel
- Copies of any parking tickets or traffic violations incurred during the period of the hire
- Evidence to prove that the cardholder had agreed to the no-show amount and terms & conditions, such as a 'Click to accept website' box

Special requirements when debiting for vehicle rental damage

In the event you experience a financial loss as a direct result of damages occurring during the cardholder's rental, you must:

- Supply written confirmation to the cardholder within 10 business days of the return date of the vehicle, informing the cardholder of the damage and cost of repairs.
- The cardholder has the right, within 10 business days of the receipt of the communication, and at no cost to the vehicle rental company, to provide an alternative estimate for the cost of repairing the damage should they choose to do so.
- If an agreement is not reached the Cardholder retains the right to raise a chargeback.
- The vehicle rental company must wait 20 business days from the original confirmation letter, before processing the delayed or amended charge and the charge must be processed within 90 days of the date of the original transaction.

Transactions that are processed in other ways, such as deposit transactions that are withheld after the vehicle hire, are likely to be disputed through the chargeback process and may result in a financial loss to your company.

Disputes (including chargebacks) on Visa cards

In the event that we receive a disputed Visa card transaction, we will write to you requesting documentation to assist us in defending the dispute. Should the documentation not be supplied to us within the timescale indicated in the letter this will result in a chargeback debit to your bank account.

When you reply you must supply:

- A dated copy of the original notification letter sent to the cardholder informing them of the delayed or amended charge that they incurred
- A copy of the original rental agreement
- An estimate of the cost of repairs from an organisation that can legally provide repairs in the local currency
- Documentation to support the billing amount of any parking or driving fines. The cardholder cannot be held responsible for any processing charges, or excessive charges where fines have gone unpaid and have therefore escalated.
- Relevant civil authority accident report (if applicable)
- Documentation signed by the cardholder, showing that they agree to be liable for any charge incurred during the rental period on the relevant credit card number. The cardholder signature must appear on the same page as the terms and conditions. If the terms and conditions appear on a different page of the contract, then they must be initialled by the cardholder.
- All relevant documentation must relate to the correct vehicle registration number.
- A copy of the insurance policy of the rental company, if that rental company requires that the cardholder pay an insurance deductible for damages together with a copy of the

© Worldpay 2015. All rights reserved

vehicle rental agreement showing that the cardholder consents to be responsible for the insurance deductible
- Any other documentation demonstrating cardholder liability for the damage

If you do not have this documentation, we will not be able to defend a dispute on your behalf and a chargeback debit will be processed to your bank account.

Please note that any transaction processed in a card not present environment is taken at your own risk and can be subject to a chargeback dispute resulting in a debit to your bank account.

MasterCard transactions

A charge for loss, theft or damage must be processed as a separate transaction from the underlying rental transaction. You must contact the cardholder and advise them of the loss, theft or damage and obtain authorisation from them for any additional charge you process. You should also provide the cardholder with documentation to support the charges as indicated in the Visa section above. If separate authorisation is not obtained from the cardholder it is likely that the transaction will be disputed as a chargeback resulting in a debit to your bank account.

Disputes (including chargebacks) on MasterCard's

In the event that we receive a disputed MasterCard transaction, we will write out to you requesting documentation to assist us in defending the dispute. Should the documentation not be supplied to us within the timescale indicated in the letter this will result in a chargeback debit to your bank account.

Within your reply you must supply:

- Original signed/swiped transaction receipt processed after the original rental charge
- Chip and PIN transaction receipt processed after the original rental charge
- Signed and imprinted receipt form processed after the original rental charge

If you do not have this documentation then we will not be able to defend a dispute on your behalf and a chargeback debit will be processed to your bank account.
Please note that any transaction processed in a card not present environment is taken at your own risk and can be subject to a chargeback dispute resulting in a debit to your bank account.

16.3 Bureau de Change

If you operate as a bureau de change, you can offer your customers the flexibility to exchange currency and pay by card for a range of different currencies, including Sterling. If you offer both travel agency and bureau de change facilities, you must have separate Customer Numbers and terminals for each facility.

16.3.1 Important extra instructions

To process bureau de change transactions, you must follow the instructions for card present transactions, as well as those listed below.

16.3.2 The basics

- Your floor limit is zero so you will always need to obtain authorisation.
- You cannot accept Maestro cards.
- Always advise the cardholder that their card issuer may charge a cash-handling fee.
- You must ensure that the additional identity checks are fully completed.

© Worldpay 2015. All rights reserved

16.3.3 Additional identity checks

- Before starting the transaction, ask the cardholder for a second form of identification (ID) – even if the payment card has their photograph on it.
- This secondary ID must be a current official government document, such as a passport or a full (not provisional) driving licence, showing the cardholder's signature. Do not accept any other ID. The document must be current and not out of date.
- If your customer does not have acceptable secondary ID, you must not go ahead with the transaction. Failure to undertake a secondary ID check may lead to chargebacks if cardholders dispute the transaction.
- Examine the secondary ID carefully for changes to photographs and signatures.
- Write full details of the secondary ID on the front of the point-of-sale (POS) receipt.
- These details should include: serial number, expiry date, jurisdiction of issue, and the holder's name (if it appears in a different format from that on the card) and address. Never abbreviate this information – it's not acceptable to write "DL" for driving licence or "P No" for Passport Number. If you write abbreviations and the transaction is later proven to be fraudulent, there may be a chargeback.

16.3.4 Additional payment card checks

- The four-digit code, printed above or below the embossed account number on the face of the card, must match the first four digits of the account number.
- Write this four-digit code on the front of the point-of-sale (POS) receipt with the words "card prefix" before it.
- If you have a UV lamp, put the card under it and check the appropriate in-built security feature. Examples can be found in our Card Recognition Guide in Section 17.
- You can also use a UV lamp to view the in-built security features of any UK driving licence used as secondary ID.

16.3.5 American Express and JCB

Please use the separate instructions provided by these card companies.

16.4 myCurrency

If your business has a high number of international customers then you could benefit from myCurrency –an innovative service that gives your customers the option of paying in their own currency. Simply use it through your terminal which will recognise when an overseas-issued card is being used and give the cardholder the option to pay in their own currency. You will receive the payment in Sterling as usual.

For further information please visit our myCurrency website.

16.5 Tax free shopping

If your business has a high number of international customers you can increase your service offering and enjoy a new source of income. Our terminal-based service plus Global Blue's expert support and extensive refund network makes tax free shopping easy for you and your high-spending international customers.

For further information please visit our Tax free shopping website

© Worldpay 2015. All rights reserved

17 Card Recognition Guide

The majority of cards you see will be processed as chip and PIN or contactless and will not require you to have sight of the card. However, if the transaction is not completed by entering PIN or the card is a signature-only card, you will need to verify that the signature on the receipt matches that on the card. As more and more cards are introduced into the marketplace, you will be presented with cards of various shapes, sizes and colours. Provided you ensure that all the security features are present, including those specific to the individual card schemes, you can accept the card for payment.

We recommend that all your staff know the process for accepting card payments, be familiar with these security features and always follow the prompts on your terminal.

17.1 Not a chip and PIN card or Contactless card?

Most cards are now chip and PIN and/or Contactless enabled, but you may sometimes be presented with chip and signature or magnetic swipe and signature cards. You must accept these cards as long as you verify the card and ensure that it has all the security features explained in this section, including those specific to the individual card schemes.

17.2 Key security features

As cards are normally placed in or tapped against card readers by the cardholder, you may not have the opportunity to check all of these security features, but these are the key details to check if you have any suspicions.
Note that not all cards are embossed or have a full account number or cardholder name, but genuine cards will always have a:

- **Card logo** – see examples below
- **Hologram** – see examples below
- **Ultraviolet image**
- **Card Security Code (CSC)** - A three-digit code at the end of the signature strip or in a separate white box next to it. American Express cards have a four-digit CSC on the front.

17.3 Example cards

To see images and details of example cards please connect directly to the applicable Card Scheme web sites or view the sample Visa card below

MasterCard
http://www.mastercard.com/uk/merchant/en/security/datasecurityrules/card_id_sec_features.html

Diners/Discover
http://www.dinersclub.com/assets/DinersClub_card_ID_features.pdf

JCB
http://partner.jcbcard.com/acceptance/holographicstripe.html

© Worldpay 2015. All rights reserved

American Express
https://web.aexp-static.com/sg/content/merchant/pdf/working-with-us/avoiding-card-fraud/check-card-faces/Guide_to_checking_Card_Faces.pdf

Visa

Card Front Card Rear

1. Chip
2. Primary Account Number (PAN)
3. First four digits repeated
4. Cardholder name
5. Expiry date, valid from date if shown
6. Contactless Wave indicator
7. Card scheme logo
8. Hologram
9. Signature strip
10. Card Security Code (CSC)

17.4 What to look out for?

17.4.1 Chip

If there is a chip; check if there is any visible damage.

17.4.2 Card number

The card number – the long number on the front – should be clear, even and in line.

17.4.3 The first four digits of the card number

Will be laser-imprinted on the front of the card beside the embossed details and should be identical to the embossed details (smaller type, above or below the beginning of the long embossed number).

17.4.4 Cardholder title and name

Should be clear, even and in-line. Embossed cards must have either a cardholder name or description such as ‘club member’ or ‘gift card’, etc. For flat-printed cards the cardholder name or description is optional.

Check that the title and name on the card match the gender of the person presenting it.

© Worldpay 2015. All rights reserved

17.4.5 Expiry date/valid from date

All cards have an expiry date, but only some have a valid from date. Check that the card isn't being presented before its 'valid from' date or after its expiry date.

17.4.6 Contactless indicator

This 'wave' symbol indicates that the card can be used to make payments without swiping it or inserting it into a terminal. This symbol usually appears on the front of the card.

17.4.7 Card scheme logo

To download Card Scheme logos, please download directly from the Card Scheme web sites using the applicable links below.

Visa – http://www.visaeurope.com/en/newsroom/video_library/images/all_images.aspx

MasterCard/Maestro - http://www.mastercardbrandcenter.com/us/index.shtml

JCB – http://partner.jcbcard.com/acceptance/jcblogo.html

Diners/Discover – http://www.dinersclub.com/press-room/acceptance-logos.html

Amex - https://www209.americanexpress.com/merchant/marketing-data-intl/emea/en_GB/pages/home

17.4.8 Hologram

These may be on the front or back of the card. The 3D image should move when the card is tilted. If the Visa logo has been placed on the back of the card it will usually be a miniature version.

These are the most common holograms currently in use:

- **MasterCard** – the world(/globe)
- **Visa** – a dove, which appears to fly
- **Maestro (UK-issued)** – William Shakespeare's head
- **Visa Electron** – not all these cards have a hologram. If there is one, it will be a flying dove.

17.4.9 Signature strip

The signature strip should not stand proud of the card. Check that either the full card number or the last four digits of the card number are printed in reverse italic text on the signature strip. However, if the transaction is not completed by entering the PIN or the card is a signature-only card, you will need to verify that the signature on the receipt matches that on the card.

© Worldpay 2015. All rights reserved

17.4.10 Card Security Code (CSC)

Usually on the reverse of the card, either on the signature strip or in a white box to the side of the signature strip.

17.5 Visa combination cards

These cards allow cardholders to choose how they pay – for example, by debit or credit account. When the customer offers the card, they choose which function they want to use. Combination cards look very much like regular Visa cards but have:

- Two card numbers, one of which is printed on the back of the card
- Two three-digit security codes
- A description of the different functions on some cards, near the Visa logo

The processes to follow when accepting a combination card are the same as for all other cards except that the terminal will prompt for a decision to be made about the function to use for the transaction.

17.6 Examples of card UV images

If an ultraviolet lamp is available place the card under and check for the appropriate mark. **Note** - Some Visa Electron cards do not carry UV features:

© Worldpay 2015. All rights reserved

18 Terminology

3D Secure – see Cardholder Authentication

A

Acquirer – A financial institution that is a member of the Card Schemes and provides facilities for businesses to accept card payments and receive these funds. Also known as a 'card acquirer'.

Address Verification Service (AVS) – Fraud-prevention service that verifies the numerical elements of a customer address against a card.

Approved Scan Vendor (ASV) – A provider approved by the PCI Security Standard Council to carry out a Vulnerability Scan of your systems. Should be contacted as part of the PCI DSS compliance process if external vulnerability scans are required.

A list is available from https://www.pcisecuritystandards.org/.

Find out more in Payment and Information Security. See section 3.

Authorisation – The process whereby a transaction for a specified amount is approved or declined by a card issuer or an acquirer on behalf of a card issuer. This approval confirms that the card number is valid, that as at the time of the transaction the card has not been reported lost or stolen and that funds were available. **It does not confirm the authenticity of the card presenter or the card, or guarantee settlement of the transaction.**

The authorisation request may be generated by a customer terminal and processed electronically or may include voice contact between the customer and the acquirer. Find out more about Authorisation and Referrals . See section 5.

Authorisation Call – A telephone call made to obtain authorisation for a transaction.

Authorisation Code – A code (which must not be all zeros) generated by a card issuer or by an acquirer on behalf of a card issuer when an authorisation request is approved. Find out more about Authorisation and Referrals. See Section 5.

B

Banking Summary Vouchers – Only needed if you are using paper vouchers. Find out more in Terminal Failure. See section 8.

Batch – A collection of transactions held at a single terminal or outlet. A batch may contain any number of shifts or days data.

Batch Totals – Find out about these in Reconciling Your Invoice.

C

Card Acquirer – See Acquirer.

Card Issuer – The organisation that issues a payment card to the cardholder.

Card Not Present Transactions – Card payments processed when the card and cardholder are not present during a transaction.

Card Number – The long number across the front of a card, also known as the PAN (Primary Account Number).

Card Present Transactions – Card payments processed where both the card and cardholder are present during a

© Worldpay 2015. All rights reserved

transaction.

Card Processing Facility – The agreed products and services provided by Worldpay which allow you to accept and process card payments.

Card Schemes – Visa, MasterCard, American Express, Diners/Discover, JCB (Japan Credit Bureau).

These independent organisations have set up systems for issuing and accepting card payments worldwide, some using local financial institutions as agents.

Card Security Code (CSC) – This is a three-digit code at the end of the signature strip or in a separate white box next to the signature strip on a card. American Express cards have a four-digit CSC on the front of the card. **Never record the CSC – it must only be used for one transaction.** The Card Security Code (CSC) is sometimes also called the Card Verification Value (CVV or CVV2) or Card Verification Code (CVC or CVC2).[1]

Card Testing – When a fraudster places an order over the phone or online to check if the card details they have will be authorised. Find out more in Reducing Fraud. See section 13.

Card Verification Code (CVC or CVC2) – Refer to Card Security Code

Card Verification Value (CVV or CVV2) – Refer to Card Security Code

Cardholder – The person to whom a card is issued, or an individual authorised to use the card.

Cardholder Authentication – Worldpay Cardholder Authentication is a security tool designed to help you authenticate cardholder details in the online eCommerce environment. It brings together MasterCard SecureCode (SecureCode) and Verified by Visa (VbV) and is also referred to as '3D Secure'.

Cardholder Data – The data obtained as part of a transaction, including:

- PAN / card number
- Cardholder's name
- Expiry date
- Service Code
- Sensitive Authentication Data

Chargeback – The term used where a card issuer can reverse part or all of the value of a transaction back to you as a merchant via the acquirer which processed the transaction, for example, when a transaction is disputed because it is proven to be fraudulent or because the customer has not followed the correct procedures. Find out more in Chargebacks. See Section 15.

Chip and PIN – Chip and PIN is a programme aimed at reducing fraud for those transactions where the cardholder and card are present at the time of the transaction.

The chip (silver or gold coloured square on the front left side of the card) is embedded into a card to provide highly secure memory and processing capabilities. In addition to holding the same personal data as the magnetic stripe, the chip provides additional security features to safeguard against counterfeiting.

The PIN is a four-digit number that the cardholder enters into the PIN pad instead of signing a card receipt. Liability for counterfeit card transactions and lost and stolen card fraud now stands with the party in any transaction who is not chip and PIN compliant. Where all parties are compliant, counterfeit transactions are reduced significantly and there will be no recourse by the cardholder saying they did not authorise the transaction.

'Code 10' Call – A call made to the Authorisation Centre if you are suspicious about a transaction. Find out more in Authorisation and Referrals .See Section 5.

Compromise – Intrusion into computer systems where unauthorised disclosure, modification or destruction of cardholder data is suspected.

© Worldpay 2015. All rights reserved

Contract – Your formal agreement with Worldpay.

Credit Card – A payment card linked to an account which may be settled in full by a set date or repaid over a period of time, subject to minimum monthly repayments being made. Interest will normally be charged to the cardholder on any outstanding balance. Examples of credit cards include MasterCard and Visa.

Customer Number – The unique number you are given when you sign a contract with us which identifies your business on our systems. This is also known as the Merchant ID (MID).

D

Data Controller - The Information Commissioner's Office website defines this role as:

- *"...a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed."*

Debit card – A card that enables a customer to transfer money from a current account or other similar account to make a payment. Examples of debit cards include Maestro, Debit MasterCard and Visa Debit.

E

eCommerce Transaction – A sale made over the Internet. You need a special agreement with us to handle these transactions.

Encryption – A way of converting information into an unintelligible format that allows storage or transmission of data without compromise.

Express Checkout – A service available to hotel businesses. Find out more in Hotel Services. Section 16.1.

F

Firewall – Hardware, software, or both that protects data on a network or computer from intruders from other networks. Typically, an enterprise with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources.

Floor Limit – An amount agreed between Worldpay and our customer for a single transaction over which authorisation and approval must be obtained. Floor limits above zero are only available for face-to-face chip card transactions.

Any transactions over the agreed floor limit will require authorisation to be obtained.

- In most instances floor limits will be set at zero. However, depending on the nature of your business, you may have different floor limits for transactions on your terminal, transactions using paper vouchers and for any card not present transactions. Details of your floor limits can be found in your Worldpay Contract.
- Make sure all your employees know the right floor limit for each type of sale, but do not write floor limits down where customers can see them, or tell customers what they are.
- Your electronic terminal has pre-programmed floor limits and will automatically telephone for authorisation when necessary.
- The floor limit applies even if the cardholder asks to pay part in cash and part by card. If the total amount of the transaction is over your floor limit, telephone for authorisation – even if the card payment amount is below the limit. Tell the Authorisation Centre that it is a 'split sale'.

Forensic Investigation – Investigation carried out under scientific procedures, with or without police involvement. This can involve removal of computer equipment and data storage from your premises.

© Worldpay 2015. All rights reserved

G

Guaranteed Reservation – A service available to hotel businesses. Find out more in Hotel Services. Section 16.1

M

Magnetic Stripe Data ('Track Data') – Data encoded in the magnetic stripe on the back of cards which is used for authorisation during transactions when the card is presented. For chip and PIN transactions, the terminal uses equivalent data contained on the chip – this data should not be retained.
Mail Order Telephone Order (MOTO) – Transaction where the order and card details are taken over the telephone or by post. Find out more in Mail Order Telephone Order Transactions. Section 10.

Management Information (MI) – Reports and analysis for monitoring your transaction processing and charges. Find out more in Reconciling Your Invoice .Section 13.

MasterCard SecureCode – see SecureCode.

Merchant ID (MID) – See Customer Number.

Merchant Operating Instructions – The original name for this guide which we are now referring to as our Customer Operating Instructions.

N

Network – A network exists if two or more computers are connected.

P

Paper Vouchers – Used for manual payment processing. Only to be used in emergencies - see Terminal Failure, section 8.

Password – A mixture of characters that can be used to authenticate an individual, allowing them access to a system, computer or network.

Payment Card – A generic term for any plastic card – credit, debit, charge and so on – which may be used on its own to pay for goods and services, or to withdraw cash.

Payment Card Industry Data Security Standard (PCI DSS) – A compliance requirement that aims to ensure that cardholder information is always stored, processed and transmitted securely.

Payment Card Industry Security Standards Council (PCI SSC) An organisation founded by five global payment brands - American Express, Diners/Discover, JCB International, MasterCard Worldwide and Visa Inc.

Payment Gateway – This is your 'virtual cash till' for eCommerce transactions.

Payment Service Provider (PSP) – PSP's offer retailers online services for accepting eCommerce (internet) payments by a variety of payment methods including cards.

PCI SSC ISA - Payment Card Industry Security Standards Council Internal Security Assessor.

Personal Identification Number (PIN) – A set of digits (usually four) entered by the cardholder to authenticate a chip & PIN transaction.

Primary Account Number (PAN) – The cardholder number of up to 19 digits which is usually, although not always, embossed on the front of the card.

© Worldpay 2015. All rights reserved

Prioritised Approach – Now a mandatory risk-based process that must be followed by all PCI Level 1-3 customers. The Prioritised Approach provides guidance on how to focus PCI DSS compliance work in a way that ensures prioritising the highest security risks.

Purchase With Cash Back (PWCB) – An optional transaction type where a customer may, with the approval of Worldpay, allow a cardholder to draw cash up to an agreed limit as part of a standard sale transaction. This is also known as 'cash back'. Find out more about Purchase with Cash Back. See Section 7.

Q

Qualified Security Assessor (QSA) – These organisations are trained on PCI DSS by the PCI Security Standards Council and can confirm a customer's compliance status or simply offer support in reaching compliance.

QSA – Qualified Security Assessor – The PCI Security Standards Council maintains a list of all persons qualified to assess your systems and processes.
For a list, see https://www.pcisecuritystandards.org/.

R

Reconciliation – The method by which a customer compares the business undertaken at their terminal with that recorded by the acquirer and credited to their bank account.

Recurring Transactions – Transactions that are authorised by a customer to be submitted at regular intervals (i.e., weekly, monthly, quarterly, etc.) and on a predetermined basis.

Referral – When your terminal prompts you to make a manual authorisation call.

Request for Information (RFI) – A request by either the card issuer or the cardholder for further information about a transaction.

S

Secondary Identification (ID) – Additional identification that the cardholder may need to produce to prove their identity. This is usually a current government document with a photograph and address. Find out more in Reducing Fraud. Section 13

SecureCode (or MasterCard SecureCode) – A method introduced by MasterCard to provide an additional, secure cardholder verification process prior to an eCommerce transaction proceeding over the Internet.

Self-Assessment Questionnaire (SAQ) – Part of the Payment Card Industry Data Security Standard (PCI DSS) compliance process. Validation tool intended to assist customers and service providers in self-evaluating their compliance with the PCI DSS. You can download the appropriate version from the SSC website.

Sensitive Authentication Data (SAD) – This is defined as full magnetic stripe data, CAV2/CVC2/CVV2/CID and PINs/PIN blocks – this data should not be retained by the customer.

Service Code – Messages contained within a card's magnetic stripe or chip that tells a terminal which process to follow for a transaction.

Service Provider – Business entity that is not a payment card brand member or a retailer directly involved in the processing, storage, transmission and switching of transaction data, cardholder data or both.

Split Sale/Transaction –Where a sale is split into two (or more) **separate amounts on one (or more) card/s in order to avoid obtaining authorisation for the full amount on one card**

© Worldpay 2015. All rights reserved

Supervisor Code – Code set by terminal manufacturer. These are freely available, so all codes should be personalised and changed regularly to prevent compromise.

T

Terminal Receipt – The paper receipt that is printed when a transaction is completed.

Terminal User Guide – The instructions that came with your terminal. It is important to read these carefully together with these Customer Operating Instructions.

Top-up Authorisation – You will need top-up authorisation on pre-authorised transactions where the amount of the final transaction is more than 15% higher than the original pre-authorised amount.

'Track Data' – Information about the card and cardholder that is kept in the card's magnetic stripe or chip. (See also 'Magnetic Stripe Data').

Transaction – A card payment in exchange for goods or services that you are providing falling within the nature of business you described to us in your application form or which you subsequently notified us of in writing.

Transaction Amount – The full amount the customer pays for the goods or services, including any VAT.

Transaction Data – Information that identifies the purchases a cardholder makes with their card.

V

Verified by Visa (VbV) – A method introduced by Visa to provide a secure cardholder verification process for eCommerce transactions.

Vulnerability Scan – Externally-facing scans of your Internet-facing IP addresses that check for unknown vulnerabilities in your network.

W

Written Authority Form – The form your customer needs to complete to authorise you to take recurring transactions from their card. Find out more in Recurring Transactions. Section 12.

© Worldpay 2015. All rights reserved